NSA-2401

Network Storage Appliance

User's Guide

Version 1.10
3/2009
Edition 1

DEFAULT LOGIN	
LAN1 IP Address	**192.168.1.3**
LAN2 IP Address	**192.168.100.3**
Username	**admin**
Password	**1234**

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the NSA using the Web Configurator.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Web Configurator Online Help

  Embedded web help for descriptions of individual screens and supplementary information.
- Supporting Disk

  Refer to the included CD for support documents.
- ZyXEL Web Site

  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

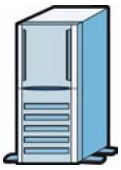
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The NSA may be referred to as the "NSA", the "device" or the "system" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The NSA icon is not an exact representation of your device.

NSA	Computer	Notebook computer
Server 	Firewall	Switch
Router		

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- ONLY qualified service personnel should service or disassemble this device.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: RISK OF EXPLOSION IF BATTERY (on the motherboard) IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS. Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Contents Overview

Introduction and Tutorials 29

Getting to Know Your NSA 31
Introducing the Web Configurator 35
Tutorials 55

Web Configurator 115

Status Screen 117
System Setting Screen 121
Storage Screens 125
Network Screens 159
Sharing Screens 173
Protect Screens 197
Application Screens 223
Maintenance Screens 229

Troubleshooting and Specifications 247

Troubleshooting 249
Product Specifications 257

Appendices and Index 263

Table of Contents

About This User's Guide 3

Document Conventions 4

Safety Warnings 6

Contents Overview 9

Table of Contents 11

List of Figures 17

List of Tables 25

Part I: Introduction and Tutorials 29

Chapter 1
Getting to Know Your NSA 31

1.1 NSA-2401 Overview 31
1.1.1 Front Panel LEDs 32
1.1.2 Power Button 33
1.1.3 COPY Button 33

Chapter 2
Introducing the Web Configurator 35

2.1 Web Configurator Overview 35
2.2 Accessing the NSA Web Configurator 35
2.2.1 Access the NSA Using the NDU 35
2.2.2 Web Browser Access 36
2.3 Login 36
2.4 User-level Screens Overview 37
2.5 My NSA Screen 38
2.5.1 My NSA Share Browsing Screen 40
2.5.2 My NSA Share Browsing Move to or Copy to Screen 42
2.5.3 My NSA Share Configuration 42
2.5.4 My NSA Change Share Properties Screen 43
2.5.5 Share and Folder Names 45
2.5.6 Share Paths 46
2.5.7 Password Screen 46

2.6 Administration Screens 47
2.6.1 Global Administration Icons 48
2.6.2 Navigation Panel 49
2.6.3 Main Window 51
2.6.4 Status Messages 51
2.6.5 Common Screen Icons 51
2.7 NSA RESET Button 52
2.7.1 Reset 52
2.7.2 Reload Factory Default Configuration File 52

Chapter 3
Tutorials 55

3.1 Overview 55
3.2 How to Configure Sharing 55
3.2.1 Setting Up User Accounts 55
3.2.2 Setting Up Groups 58
3.2.3 Setting Up Shares 59
3.3 How to Use Shares 61
3.3.1 Using a Share with Windows Explorer 61
3.3.2 Using a Share with a Web Browser 62
3.4 How to Find the NSA in OS X 65
3.5 How to Configure Security 68
3.5.1 Configuring Security for Web Configurator Sessions 68
3.5.2 Using FTPES to Connect to the NSA 81
3.5.3 Controlling Access to Shares, Folders, and Files 83
3.6 Power Resume 89
3.7 How to Use Backups and Snapshots 89
3.7.1 Creating a Snapshot Job 90
3.7.2 Configuring Snapshot Image Access 91
3.7.3 Using a Snapshot Image to Restore Files 91
3.7.4 Creating a Synchronization Backup 92
3.7.5 Creating an Archive Backup 96
3.7.6 Restoring Archived Files by Backup Job 99
3.7.7 Restoring by Backup Files 102
3.8 Printer Server Tutorial 104
3.9 How to Increase the NSA's Storage Capacity 106
3.9.1 Connecting External USB Hard Drives 107
3.9.2 Adding an Internal Hard Drive to an Existing Disk Array 107
3.9.3 Using a Disk Array's Increased Capacity 109
3.9.4 Migrating a RAID to Higher Capacity Hard Drives 110

Part II: Web Configurator 115

Chapter 4
Status Screen 117

4.1 Status Screen 117

Chapter 5
System Setting Screen 121

5.1 Date/Time 121
5.1.1 Time Lag 122

Chapter 6
Storage Screens 125

6.1 Storage Screens Overview 125
6.1.1 What You Can Do in the Storage Screens 125
6.1.2 What You Need to Know About Storage 125
6.2 Internal Storage Status Screen 127
6.3 Disk 128
6.3.1 Internal Disks Screen 128
6.3.2 S.M.A.R.T Screen 129
6.4 Arrays 132
6.4.1 RAID Levels 132
6.4.2 Array Status 134
6.5 RAID Screen 135
6.5.1 Creating a New RAID 138
6.6 Internal Volume Screen 139
6.6.1 Creating or Editing an Internal Volume 142
6.6.2 USB Key Creation 143
6.7 External Storage Disk Screen 145
6.8 External Volume Screen 147
6.8.1 Creating or Editing an External Volume 149
6.9 Technical Reference 151
6.9.1 Storage Terminology 151
6.9.2 JBOD 152
6.9.3 RAID 0 153
6.9.4 RAID 1 153
6.9.5 RAID 10 154
6.9.6 RAID 5 155
6.9.7 Hot-spare 155
6.9.8 RAID and Data Protection 156
6.9.9 S.M.A.R.T Attributes 156

Chapter 7
Network Screens 159

7.1 Network Screens Overview 159

7.1.1 What You Can Do in the Network Screens 159
7.1.2 What You Need to Know About the Network Screens 159
7.2 TCP/IP Screen 160
7.2.1 Configuring the TCP/IP Screen 162
7.3 Windows/CIFS 164
7.3.1 Windows/CIFS Screen 166
7.4 NFS Screen 168
7.4.1 Add or Edit NFS Share Screen 169
7.4.2 NFS Session Screen 170

Chapter 8
Sharing Screens 173

8.1 Overview 173
8.1.1 What You Can Do In The Sharing Screens 173
8.1.2 What You Need to Know About The Sharing Screens 173
8.2 Users 175
8.2.1 Create a New Account & Change Account Properties 178
8.2.2 View User Information 181
8.3 Groups 182
8.3.1 Add a New Local Group & Change Group Properties 184
8.4 Shares 186
8.4.1 Create a New Share & Edit a Share 188
8.4.2 ACL Configuration 190
8.4.3 Recycle Bin 194
8.4.4 DFS 194

Chapter 9
Protect Screens 197

9.1 Protection Methods Overview 197
9.1.1 What You Can Do in the Protect Screens 198
9.1.2 What You Need to Know About Protection Methods 198
9.2 NSA Backup Screens 200
9.2.1 Backup Summary 200
9.2.2 Creating a Backup Job 202
9.2.3 Editing a Backup Job 208
9.2.4 Restoring by Backup Job 209
9.3 Restoring by Backup Files 212
9.3.1 Protect > Restore: Step 2 213
9.3.2 Protect > Restore: Step 3 214
9.3.3 Protect > Restore: Step 4 215
9.4 Snapshots 215
9.4.1 Creating/Editing Snapshots 218
9.4.2 Snapshot Images 219

9.5 Backup Software Screen 220

Chapter 10
Application Screens 223

10.1 Overview 223
10.1.1 What You Can Do In The Application Screens 223
10.1.2 What You Need to Know About The Application Screens 223
10.2 FTP 224
10.3 Print Server 226
10.3.1 Print Server Rename 226
10.4 Copy Button 227
10.4.1 Changing the Copy Button Share 227

Chapter 11
Maintenance Screens 229

11.1 Overview 229
11.1.1 What You Can Do In The Maintenance Screens 229
11.1.2 What You Need to Know About The Maintenance Screens 229
11.2 Log 230
11.2.1 Search 232
11.2.2 Log Records Configuration 232
11.2.3 Log Buzzer Priority Configuration 233
11.2.4 Report Configuration 233
11.2.5 Export Log 236
11.3 Configuration 237
11.3.1 Restoring the Configuration File 238
11.4 SSL 239
11.5 Firmware Upgrade 241
11.6 Power Management 242
11.6.1 Power Control Schedule 244
11.7 Shutdown 245

Part III: Troubleshooting and Specifications 247

Chapter 12
Troubleshooting 249

12.1 Troubleshooting Overview 249
12.2 Power, Hardware Connections, and LEDs 249
12.3 NSA Login and Access 251
12.4 Users Cannot Access the NSA 253
12.5 Backups and Snapshots 254

12.6 External USB Disks 255

Chapter 13
Product Specifications 257

13.1 Feature Tables 257
13.2 Specification Tables 259
13.3 Power Consumption 261

Part IV: Appendices and Index 263

Appendix A Log Messages 265

Appendix B Setting Up Your Computer's IP Address 275

Appendix C Importing Certificates 299

Appendix D Open Source Licences 323

Appendix E Legal Information 353

Index 355

List of Figures

Figure 1 NSA Overview 31
Figure 2 NSA Front Panel LEDs 32
Figure 3 NDU Main Screen 36
Figure 4 NDA URL 36
Figure 5 NSA Login Screen 37
Figure 6 Change Password Screen 37
Figure 7 My NSA 38
Figure 8 My NSA Screen 39
Figure 9 My NSA Share Browsing 40
Figure 10 My NSA Share Browsing > Move to (or Copy to) 42
Figure 11 My NSA Share Configuration 42
Figure 12 My NSA Change Share Properties 43
Figure 13 My NSA Change Share Properties > Share Access Configuration 45
Figure 14 Password 46
Figure 15 Status 48
Figure 16 Navigation Panel Links 49
Figure 17 Reset and Reload Timeline 53
Figure 18 Administrator Login 56
Figure 19 My NSA 56
Figure 20 Sharing > Users 57
Figure 21 Sharing > Users > Create a New Account 57
Figure 22 Groups 58
Figure 23 Sharing > Groups > Add Share 59
Figure 24 Shares 59
Figure 25 Sharing > Shares > Add Share 60
Figure 26 Share Access Configuration 60
Figure 27 Sharing > Shares > Add Share 61
Figure 28 Mapping a Share 61
Figure 29 Entering the Share Username and Password 62
Figure 30 Creating a Folder 62
Figure 31 Using the Folder 62
Figure 32 User Login 63
Figure 33 Gonzo's My NSA Screens 63
Figure 34 Gonzo Share Screen 64
Figure 35 Strategy Folder Screen 65
Figure 36 Upload Files Screen 65
Figure 37 Opening the Finder 66
Figure 38 Displaying the NSA 66

Figure 39 Displaying the NSA 67
Figure 40 Alternate Method for Displaying the NSA 67
Figure 41 Connecting to the NSA 68
Figure 42 Maintenance > SSL 69
Figure 43 Maintenance > SSL > Edit a Self-Signed Certificate 69
Figure 44 Maintenance > SSL > Edit a Self-Signed Certificate 70
Figure 45 Maintenance > SSL 71
Figure 46 Downloading the NSA's Certificate 71
Figure 47 Downloading the NSA's Certificate 72
Figure 48 Certificate 72
Figure 49 Certificate Import Wizard: Welcome 73
Figure 50 Certificate Import Wizard: Certificate Store 73
Figure 51 Certificate Import Wizard: Finish 74
Figure 52 Security Warning 74
Figure 53 Certificate Import Wizard: Successful 74
Figure 54 Maintenance > SSL 75
Figure 55 Maintenance > SSL > Force HTTPS Warning 76
Figure 56 Firefox: Secure Connection Failed 76
Figure 57 Firefox: Secure Connection Failed 77
Figure 58 Firefox: Add Security Exception 77
Figure 59 Firefox: Add Security Exception 78
Figure 60 Firefox: Add Security Exception 79
Figure 61 Firefox: Add Security Exception 80
Figure 62 HTTPS Login 81
Figure 63 FileZilla Site Manager 82
Figure 64 FileZilla Unknown Certificate Warning 83
Figure 65 Sharing > Shares 83
Figure 66 Sharing > Shares > Edit Share 84
Figure 67 Share Access Configuration 84
Figure 68 Sharing > Shares 85
Figure 69 Sharing > Shares > ACL Configuration 85
Figure 70 Sharing > Shares > ACL Configuration > New ACL 86
Figure 71 Sharing > Shares > ACL Configuration > New ACL > Strategy 86
Figure 72 Sharing > Shares > ACL Configuration > New ACL > Strategy > Set ACL 87
Figure 73 Sharing > Shares > ACL Configuration > New ACL > Strategy 88
Figure 74 Sharing > Shares > ACL Configuration > New ACL > Strategy 88
Figure 75 Maintenance > Power Management 89
Figure 76 Protect > Snapshot 90
Figure 77 Protect > Snapshot > Add Job 91
Figure 78 Protect > Snapshot > Snapshot Image Access 91
Figure 79 Using a Snapshot Image 92
Figure 80 Protect > Backup 92
Figure 81 Protect > Backup > Add Job: Step 1 93

Figure 82 Protect > Backup > Add Job: Step 2 94
Figure 83 Protect > Backup > Add Job: Step 3 95
Figure 84 Protect > Backup > Add Job: Step 3 95
Figure 85 Protect > Backup > Add Job: Step 4 96
Figure 86 Protect > Backup 96
Figure 87 Protect > Backup > Add Job: Step 1 97
Figure 88 Protect > Backup > Add Job: Step 2 98
Figure 89 Protect > Backup > Add Job: Step 3 99
Figure 90 Protect > Backup > Add Job: Step 4 99
Figure 91 Protect > Backup 100
Figure 92 Protect > Backup > Restore Archive: Step 1 100
Figure 93 Protect > Backup > Restore Archive: Step 2 101
Figure 94 Protect > Backup > Restore Archive: Step 3 101
Figure 95 Protect > Backup > Restore Archive: Progress 102
Figure 96 Protect > Restore: Step 1 102
Figure 97 Protect > Restore: Step 2 103
Figure 98 Protect > Restore: Step 3 103
Figure 99 Protect > Restore: Step 4 104
Figure 100 Printer Sharing 104
Figure 101 Printer Connected to NSA: Windows Explorer 105
Figure 102 Printer Connected to NSA: Windows Explorer Warning 105
Figure 103 Printer Driver Needed 105
Figure 104 Applications > Print Server 106
Figure 105 Printer Screen in Windows Explorer 106
Figure 106 Connecting a USB Hard Drive 107
Figure 107 Storage > External Storage > Disk 107
Figure 108 Storage > Internal Storage > Disk 108
Figure 109 Storage > Internal Storage > RAID 108
Figure 110 Storage > Internal Storage > RAID > Add Disk 109
Figure 111 Storage > Internal Storage > Disk 109
Figure 112 Storage > Internal Storage > Volume 110
Figure 113 Storage > Internal Storage > Volume > Edit 110
Figure 114 Storage > Internal Storage > Disk 111
Figure 115 Storage > Internal Storage > Disk > Eject 111
Figure 116 Storage > Internal Storage > Disk > Eject 111
Figure 117 Status: RAID Degraded 112
Figure 118 Storage > Internal Storage > RAID 112
Figure 119 Storage > Internal Storage > RAID > Repair 112
Figure 120 Storage > Internal Storage > RAID 113
Figure 121 Status Screen 117
Figure 122 System Setting > Date/Time 121
Figure 123 Disks, RAIDs, and Volumes 125
Figure 124 Storage > Internal Storage > Status 127

Figure 125 Storage > Internal Storage > Disk 128
Figure 126 Storage > Internal Storage > Disk > S.M.A.R.T. (Brief Summary) 130
Figure 127 Storage > Internal Storage > Disk > S.M.A.R.T. (Full Summary) 131
Figure 128 Storage > Internal Storage > RAID 135
Figure 129 Storage > Internal Storage > RAID > Create 138
Figure 130 Storage > Internal Storage > Volume 140
Figure 131 Storage > Internal Storage > Volume > Create 142
Figure 132 Selecting the USB Device 144
Figure 133 Creating a Duplicate USB Key 144
Figure 134 Creating a Duplicate USB Key: Eject 145
Figure 135 Creating a Duplicate USB Key: Insert 145
Figure 136 Storage > External Storage > Disk 145
Figure 137 Storage > External Storage > Volume 147
Figure 138 Storage > External Storage > Volume > Create 149
Figure 139 Stand Alone Teaming Mode 160
Figure 140 Fault Tolerance Teaming Mode 161
Figure 141 Load Balancing Teaming Mode 161
Figure 142 Link Aggregation Teaming Mode 161
Figure 143 Jumbo Frames 162
Figure 144 Network > TCP/IP 163
Figure 145 Active Directory Example Application 166
Figure 146 Network > Windows/CIFS (Workgroup) 166
Figure 147 Network > Windows/CIFS (Domain) 167
Figure 148 Network > NFS 168
Figure 149 Network > NFS > Add NFS Share 169
Figure 150 Network > NFS > NFS Session 170
Figure 151 Sharing > Users 175
Figure 152 Sharing > Users > Add User 178
Figure 153 My NSA 180
Figure 154 Password 180
Figure 155 Sharing > Users > User Information 181
Figure 156 Sharing > Groups 182
Figure 157 Sharing > Groups > Add a New Local Group 184
Figure 158 Sharing > Shares 186
Figure 159 Sharing > Shares > Create a New Share 188
Figure 160 Sharing > Shares > Create a New Share > Share Access Configuration 189
Figure 161 Sharing > Shares > ACL Configuration 190
Figure 162 Sharing > Shares > ACL Configuration > New ACL Configuration 191
Figure 163 Shares > ACL Configuration > New ACL Configuration > ACL Permission 192
Figure 164 Sharing > Shares > Configuration 194
Figure 165 Sharing > Shares > DFS 194
Figure 166 Protect > Backup 201
Figure 167 Protect > Backup > Add Job: Step 1 202

Figure 168 Protect > Backup > Add: Step 2 204
Figure 169 Protect > Backup > Add Job: Step 3 206
Figure 170 Protect > Backup > Add Job: Step 4 207
Figure 171 Protect > Backup > Edit Job: Step 1 208
Figure 172 Protect > Backup > Edit Job: Step 2 209
Figure 173 Protect > Backup > Restore Archive: Step 1 210
Figure 174 Protect > Backup > Restore Archive: Step 2 211
Figure 175 Protect > Backup > Restore Archive: Step 3 211
Figure 176 Protect > Restore: Step 1 212
Figure 177 Protect > Restore: Step 2 213
Figure 178 Protect > Restore: Step 3 214
Figure 179 Protect > Restore: Step 4 215
Figure 180 Protect > Snapshot > Snapshot Jobs 216
Figure 181 Protect > Snapshot > Add Job 218
Figure 182 Protect > Snapshot > Snapshot Images 219
Figure 183 Protect > Backup Software 221
Figure 184 Printer Sharing 224
Figure 185 Applications > FTP 225
Figure 186 Applications > Print Server 226
Figure 187 Applications > Print Server > Rename 226
Figure 188 Applications > Copy Button 227
Figure 189 Applications > Copy Button > Edit 228
Figure 190 Maintenance > Log 230
Figure 191 Maintenance > Log 231
Figure 192 Maintenance > Log > Log Classes 231
Figure 193 Maintenance > Log > Search Filters 232
Figure 194 Maintenance > Log > Log Config > Log Records Configuration 232
Figure 195 Maintenance > Log > Log Config > Buzzer Priority 233
Figure 196 Maintenance > Log > Log Report Configuration > Mail Setting 234
Figure 197 Maintenance > Log > Log Report Configuration > Report Setting 235
Figure 198 Maintenance > Log > Log Report Configuration > Syslog Server Setting 236
Figure 199 Maintenance > Configuration 237
Figure 200 Maintenance > Configuration > Restore 238
Figure 201 Maintenance > Configuration > Restore > Restarting 239
Figure 202 Maintenance > SSL 239
Figure 203 Maintenance > SSL > Edit a Self-Signed Certificate 241
Figure 204 Maintenance > FW Upgrade 242
Figure 205 Maintenance > Power Management 243
Figure 206 Maintenance > Power Management > Edit 244
Figure 207 Maintenance > Shutdown 246
Figure 208 Maintenance > Shutdown > Confirm Restart 246
Figure 209 Maintenance > Shutdown > Confirm Shutdown 246
Figure 210 Power Adaptor Pinout. 261

Figure 211 Windows XP: Start Menu 276
Figure 212 Windows XP: Control Panel 276
Figure 213 Windows XP: Control Panel > Network Connections > Properties 277
Figure 214 Windows XP: Local Area Connection Properties 277
Figure 215 Windows XP: Internet Protocol (TCP/IP) Properties 278
Figure 216 Windows Vista: Start Menu 279
Figure 217 Windows Vista: Control Panel 279
Figure 218 Windows Vista: Network And Internet 279
Figure 219 Windows Vista: Network and Sharing Center 280
Figure 220 Windows Vista: Network and Sharing Center 280
Figure 221 Windows Vista: Local Area Connection Properties 281
Figure 222 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties 282
Figure 223 Mac OS X 10.4: Apple Menu 283
Figure 224 Mac OS X 10.4: System Preferences 283
Figure 225 Mac OS X 10.4: Network Preferences 284
Figure 226 Mac OS X 10.4: Network Preferences > TCP/IP Tab. 284
Figure 227 Mac OS X 10.4: Network Preferences > Ethernet 285
Figure 228 Mac OS X 10.4: Network Utility 285
Figure 229 Mac OS X 10.5: Apple Menu 286
Figure 230 Mac OS X 10.5: Systems Preferences 286
Figure 231 Mac OS X 10.5: Network Preferences > Ethernet 287
Figure 232 Mac OS X 10.5: Network Preferences > Ethernet 288
Figure 233 Mac OS X 10.5: Network Utility 288
Figure 234 Ubuntu 8: System > Administration Menu 289
Figure 235 Ubuntu 8: Network Settings > Connections 289
Figure 236 Ubuntu 8: Administrator Account Authentication 290
Figure 237 Ubuntu 8: Network Settings > Connections 290
Figure 238 Ubuntu 8: Network Settings > Properties 291
Figure 239 Ubuntu 8: Network Settings > DNS 291
Figure 240 Ubuntu 8: Network Tools 292
Figure 241 openSUSE 10.3: K Menu > Computer Menu 293
Figure 242 openSUSE 10.3: K Menu > Computer Menu 293
Figure 243 openSUSE 10.3: YaST Control Center 294
Figure 244 openSUSE 10.3: Network Settings 294
Figure 245 openSUSE 10.3: Network Card Setup 295
Figure 246 openSUSE 10.3: Network Settings 296
Figure 247 openSUSE 10.3: KNetwork Manager 297
Figure 248 openSUSE: Connection Status - KNetwork Manager 297
Figure 249 Internet Explorer 7: Certification Error 300
Figure 250 Internet Explorer 7: Certification Error 300
Figure 251 Internet Explorer 7: Certificate Error 300
Figure 252 Internet Explorer 7: Certificate 301
Figure 253 Internet Explorer 7: Certificate Import Wizard 301

Figure 254 Internet Explorer 7: Certificate Import Wizard 302
Figure 255 Internet Explorer 7: Certificate Import Wizard 302
Figure 256 Internet Explorer 7: Select Certificate Store 302
Figure 257 Internet Explorer 7: Certificate Import Wizard 303
Figure 258 Internet Explorer 7: Security Warning 303
Figure 259 Internet Explorer 7: Certificate Import Wizard 304
Figure 260 Internet Explorer 7: Website Identification 304
Figure 261 Internet Explorer 7: Public Key Certificate File 305
Figure 262 Internet Explorer 7: Open File - Security Warning 305
Figure 263 Internet Explorer 7: Tools Menu 306
Figure 264 Internet Explorer 7: Internet Options 306
Figure 265 Internet Explorer 7: Certificates 307
Figure 266 Internet Explorer 7: Certificates 307
Figure 267 Internet Explorer 7: Root Certificate Store 307
Figure 268 Firefox 2: Website Certified by an Unknown Authority 308
Figure 269 Firefox 2: Page Info 308
Figure 270 Firefox 2: Tools Menu 309
Figure 271 Firefox 2: Options 309
Figure 272 Firefox 2: Certificate Manager 310
Figure 273 Firefox 2: Select File 310
Figure 274 Firefox 2: Tools Menu 311
Figure 275 Firefox 2: Options 311
Figure 276 Firefox 2: Certificate Manager 312
Figure 277 Firefox 2: Delete Web Site Certificates 312
Figure 278 Opera 9: Certificate signer not found 313
Figure 279 Opera 9: Security information 313
Figure 280 Opera 9: Tools Menu 314
Figure 281 Opera 9: Preferences 314
Figure 282 Opera 9: Certificate manager 315
Figure 283 Opera 9: Import certificate 315
Figure 284 Opera 9: Install authority certificate 316
Figure 285 Opera 9: Install authority certificate 316
Figure 286 Opera 9: Tools Menu 317
Figure 287 Opera 9: Preferences 317
Figure 288 Opera 9: Certificate manager 318
Figure 289 Konqueror 3.5: Server Authentication 319
Figure 290 Konqueror 3.5: Server Authentication 319
Figure 291 Konqueror 3.5: KDE SSL Information 319
Figure 292 Konqueror 3.5: Public Key Certificate File 320
Figure 293 Konqueror 3.5: Certificate Import Result 320
Figure 294 Konqueror 3.5: Kleopatra 320
Figure 295 Konqueror 3.5: Settings Menu 321
Figure 296 Konqueror 3.5: Configure 321

List of Tables

Table 1 Disk Drive LEDs 32
Table 2 NSA LEDs 32
Table 3 User-level Global Labels and Icons 38
Table 4 My NSA Screen 39
Table 5 My NSA Share Browsing Icons 40
Table 6 My NSA Share Browsing 41
Table 7 My NSA Share Browsing > Move to (or Copy to) 42
Table 8 My NSA Share Configuration Icons 43
Table 9 My NSA Share Configuration 43
Table 10 My NSA Change Share Properties 43
Table 11 My NSA Change Share Properties > Share Access Configuration 45
Table 12 Password 47
Table 13 Global Labels and Icons 48
Table 14 Screens Summary 50
Table 15 Common Configuration Screen Icons 51
Table 16 Status Icons 118
Table 17 Status 118
Table 18 System Setting > Date/Time 121
Table 19 Storage > Internal Storage > Status 127
Table 20 Storage > Internal Storage > Disk Icons 129
Table 21 Storage > Internal Storage > Disk 129
Table 22 Storage > Internal Storage > Disk > S.M.A.R.T. (Brief Summary) 130
Table 23 Storage > Internal Storage > Disk > S.M.A.R.T. (Full Summary) 131
Table 24 RAID Array Levels Quick Comparison 133
Table 25 Storage > Internal Storage > RAID Icons 136
Table 26 Storage > Internal Storage > RAID 138
Table 27 Storage > Internal Storage > RAID > Create 139
Table 28 Storage > Internal Storage > Volume Icons 140
Table 29 Storage > Internal Storage > Volume 141
Table 30 Storage > Internal Storage > Volume Create 142
Table 31 Selecting the USB Device 144
Table 32 Storage > External Storage > Disk Icons 146
Table 33 Storage > External Storage > Disk 146
Table 34 Storage > External Storage > Volume Icons 147
Table 35 Storage > External Storage > Volume 148
Table 36 Storage > External Storage > Volume Create 149
Table 37 JBOD 152
Table 38 RAID 0 153

Table 39 RAID 1 153
Table 40 RAID 10 154
Table 41 RAID 5 155
Table 42 S.M.A.R.T. Attributes 156
Table 43 Network > TCP/IP 163
Table 44 Network > Windows/CIFS 167
Table 45 Network > NFS Icons 168
Table 46 Network > NFS 169
Table 47 Network > NFS > Add NFS Share 170
Table 48 Network > NFS > NFS Session 171
Table 49 Sharing > Users Icons 175
Table 50 Sharing > Users 176
Table 51 Sharing > Users > Create a New Account 178
Table 52 Sharing > Users > User Information > Quota List 181
Table 53 Sharing > Groups Icons 182
Table 54 Sharing > Groups 183
Table 55 Sharing > Groups > Add a New Local Group 184
Table 56 Sharing > Shares Icons 186
Table 57 Sharing > Shares 187
Table 58 Sharing > Shares > Create a New Share 188
Table 59 Sharing > Shares > Create a New Share > Share Access Configuration 189
Table 60 Sharing > ACL Configuration Icons 190
Table 61 Sharing > Shares > Create a New Share > Share Access Configuration 191
Table 62 Sharing > Shares > ACL Configuration > New ACL Configuration Icons 191
Table 63 Sharing > Shares > Create a New Share > Share Access Configuration 192
Table 64 Shares > ACL Configuration > New ACL Configuration > ACL Permission 193
Table 65 Shares > ACL Configuration > New ACL Configuration > ACL Permission 194
Table 66 Sharing > Shares > DFS 195
Table 67 Protection Methods Overview 197
Table 68 Protect > Backup Icons 201
Table 69 Protect > Backup 202
Table 70 Protect > Backup > Add Job: Step 1 203
Table 71 Protect > Backup > Add Job: Step 2 205
Table 72 Protect > Backup > Add Job: Step 3 206
Table 73 Protect > Backup > Add Job: Step 4 207
Table 74 Protect > Backup > Edit Job: Step 1 208
Table 75 Protect > Backup > Edit Job: Step 2 209
Table 76 Protect > Backup > Restore Archive: Step 1 210
Table 77 Protect > Backup > Restore Archive: Step 2 211
Table 78 Protect > Backup > Restore Archive: Step 3 212
Table 79 Protect > Restore: Step 1 212
Table 80 Protect > Restore: Step 2 213
Table 81 Protect > Restore: Step 3 214

Table 82 Protect > Restore: Step 4 215
Table 83 Protect > Snapshot > Snapshot Jobs Icons 217
Table 84 Protect > Snapshot > Snapshot Jobs 218
Table 85 Protect > Snapshot > Add Job 219
Table 86 Protect > Snapshot > Snapshot Images Icons 220
Table 87 Protect > Snapshot > Snapshot Images 220
Table 88 Applications > FTP 225
Table 89 Applications > Print Server 226
Table 90 Applications > Print Server > Rename 227
Table 91 Applications > Copy Button 227
Table 92 Applications > Copy Button > Edit 228
Table 93 Applications > Copy Button > Edit 228
Table 94 Maintenance > Log Icons 230
Table 95 Maintenance > Log > Search Filters 232
Table 96 Maintenance > Log > Log Config > Log Records Configuration 233
Table 97 Maintenance > Log > Log Config > Buzzer Priority 233
Table 98 Maintenance > Log > Log Report Configuration > Mail Setting 234
Table 99 Maintenance > Log > Log Report Configuration > Report Setting 235
Table 100 Maintenance > Log > Log Report Configuration > Syslog Server Setting 236
Table 101 Maintenance > Configuration 237
Table 102 Maintenance > Configuration 238
Table 103 Maintenance > SSL 240
Table 104 Maintenance > Configuration 241
Table 105 Maintenance > FW Upgrade 242
Table 106 Maintenance > Power Management 243
Table 107 Maintenance > Power Management > Edit 245
Table 108 Maintenance > Shutdown 246
Table 109 Physical Features 257
Table 110 Firmware Features 257
Table 111 NSA Hardware Specifications 259
Table 112 NSA Firmware Specifications 260
Table 113 Power Consumption in Watts (W) 261
Table 114 Log Messages 265

PART I
Introduction and Tutorials

Getting to Know Your NSA (31)
Introducing the Web Configurator (35)

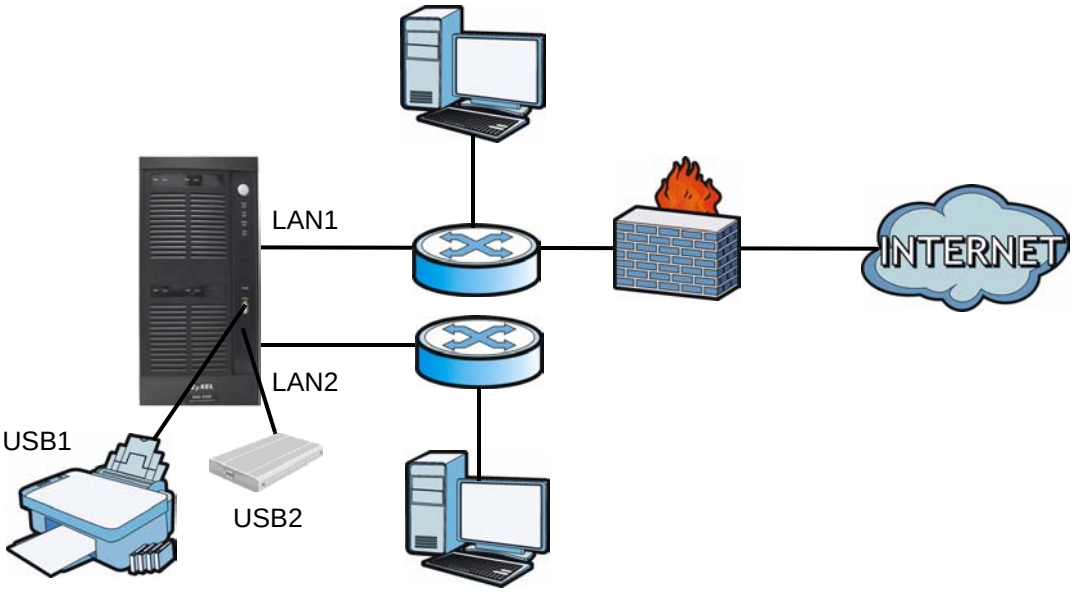
1

Getting to Know Your NSA

1.1 NSA-2401 Overview

The NSA (Network Storage Appliance) allows secure storage and management of data on your network. Windows, Apple, or Linux users can access data on it as if it was on their own computers. The NSA's two Gigabit Ethernet ports can connect to two different LANs. Users on either LAN (or connected through the Internet) can back up and share data on the NSA. Two USB ports let you share USB printers and use external USB hard drives for extra storage space.

Figure 1 NSA Overview



- The NSA's SATA II (Serial Advanced Technology Attachment) hard disk serial links are compatible with all major hard drive manufacturers.
- RAID (Redundant Array of Independent Disks) protects your data even if a hard disk fails.
- The snapshot and backup features let you further protect your data.
- The NSA offers powerful security features. Use HTTPS or FTPES for secure file transfers. Create encrypted volumes so an attacker who removes the physical drive still cannot read the data. The NSA can also record all user access to files and folders.
- The NSA lets you publish or mirror files to another NSA as a backup that others can access (at a branch office for example).
- See the specifications appendix for a more detailed list of NSA features.

1.1.1 Front Panel LEDs

The front panel LEDs tell you important information about the NSA.

Figure 2 NSA Front Panel LEDs

The following table describes the disk drive LEDs. Refer to the Quick Start Guide to see how to install and remove hard drives from the disk trays.

Table 1 Disk Drive LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	Off	The hard disk drive tray is empty or not connected properly.
		On	The hard disk drive is connected properly to the NSA.
		Blinking	The NSA is reading data from the hard disk drive or writing data to it.
ALM	Red	Off	The hard disk drive is working properly if connected.
		On	The hard disk drive has a problem, is not installed, or you have used the Web Configurator to eject it (shut it down).
		Blinking	The NSA is resynching or reshaping the hard disk drive.

The following table describes the LEDs related to the NSA itself.

The **SYS** LED blinks orange when firmware is being uploaded to the NSA. Do not turn off or reset the NSA while the firmware update is in progress!

Table 2 NSA LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	Off	The NSA is turned off.
		On	The NSA is turned on and receiving power.

Table 2 NSA LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
SYS	Red	On	The NSA has passed system tests.
		Blinking	The NSA is starting up or shutting down. Quick blinking indicates a RAID array is in degraded mode.
	Orange	On	The NSA is unlocking an encrypted volume or there are no volumes in the NSA.
		Blinking	Firmware is being uploaded to the NSA.
	Green	On	The NSA has fully booted and is operating normally.
LAN1/LAN2	Green	Off	The LAN is not connected.
		On	The NSA has a successful 10/100 Mbps Ethernet connection.
		Blinking	The 100M LAN is sending or receiving packets.
	Orange	On	The NSA has a successful 1000 Mbps Ethernet connection.
		Blinking	The 1000M LAN is sending or receiving packets.
COPY	Green	On	A USB device is connected to the NSA.
		Blinking	The NSA is copying files from the USB device.
	Red	On	Copying files from the USB device failed. Press the **COPY** button to set the **COPY** LED back to green.
		Off	No USB device is connected.

1.1.2 Power Button

Press the power button on the front panel to turn the NSA on and off.

- To turn the NSA on: press the power button and release it.
- To turn the NSA off, press the power button in and hold it until you hear a beep. Then release the button. The **SYS** light blinks red until the NSA is shut down.
- If the above shut-down procedure does not work (which may happen if the NSA has crashed), hold the power button in a few more seconds until you hear a second beep. The NSA turns off immediately.

1.1.3 COPY Button

Use the **COPY** button on the front panel to copy files from a connected USB device to the NSA. Use the **Applications** > **Copy Button** screen (Section 10.4 on page 227) to choose where the NSA stores the files. The name of the folder created for the copied files consists of the date and time of the copy in year_month_day_hour_minute_second format.

2

Introducing the Web Configurator

This chapter describes how to access the NSA Web Configurator and provides an overview of its screens.

2.1 Web Configurator Overview

The Web Configurator is an HTML-based management interface that allows easy NSA setup and management via Internet browser. Use Internet Explorer 6.0, Mozilla firefox 1.0, Netscape Navigator 7.0 or later versions of these browsers. The recommended screen resolution is 1024 by 768 pixels or higher.

In order to use the Web Configurator you need to allow JavaScripts.

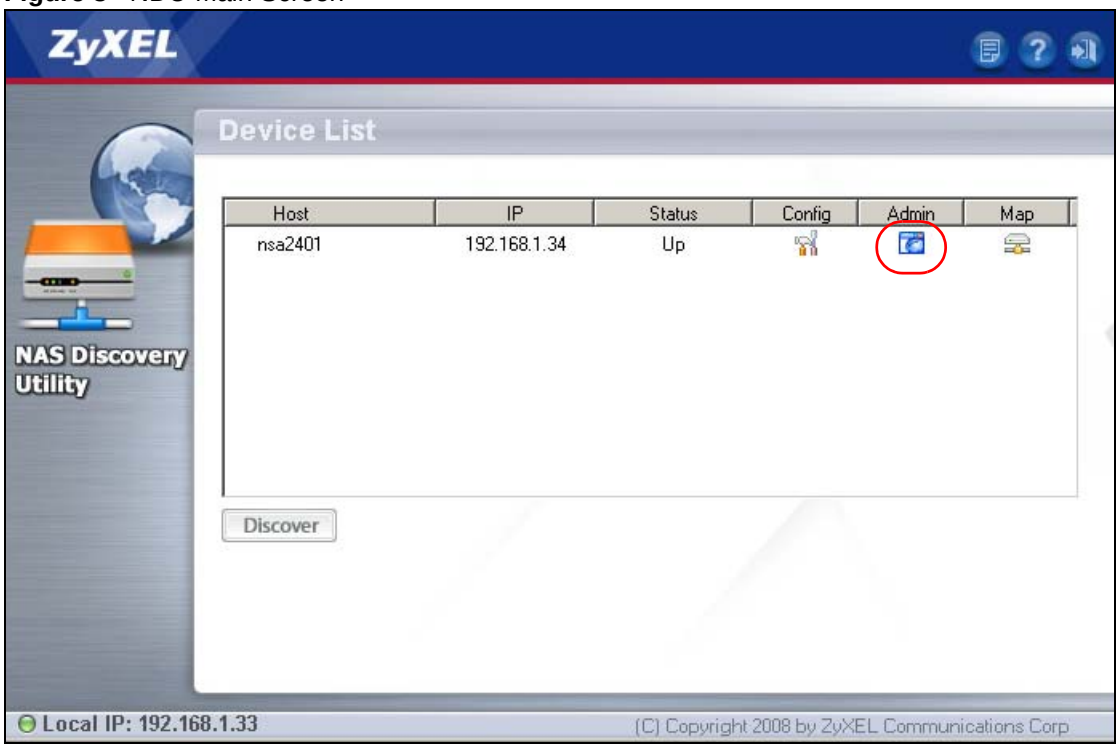
2.2 Accessing the NSA Web Configurator

Make sure your NSA is properly connected (refer to the Quick Start Guide).

2.2.1 Access the NSA Using the NDU

If you don’t know the IP address of the NSA, then use the NDU to find it. Refer to the Quick Start Guide to see how to install and run the NDU.

Figure 3 NDU Main Screen

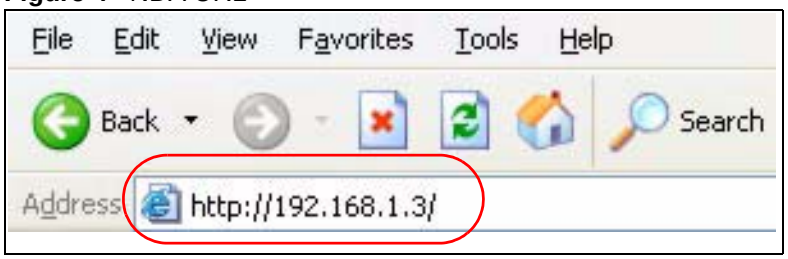


From the NDU main page click the icon under **Admin** to see the Web Configurator screen login screen.

2.2.2 Web Browser Access

Open your browser and type in the IP address of the NSA. If the NSA does not get IP addresses from a DHCP server, the default **LAN1** IP address is 192.168.1.3 and the default **LAN2** IP address is 192.168.100.3.

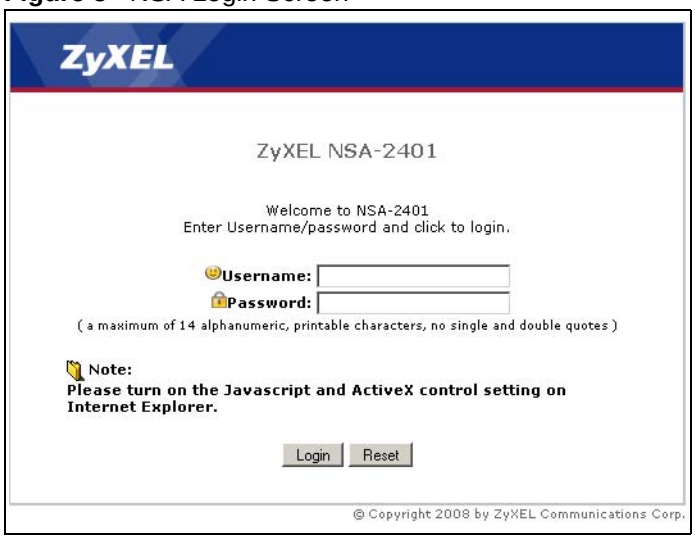
Figure 4 NDA URL



2.3 Login

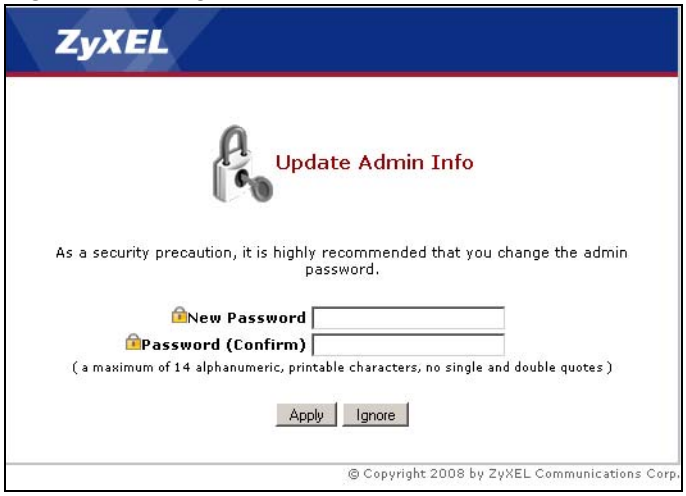
The default user name and password are ‘admin’ and ‘1234’ respectively. Enter your user name and password, then click **Login**. Non-admin users can change their passwords by using the username and password in the **My NSA** > **Password** screen. See Section 2.5.7 on page 46 for details.

Figure 5 NSA Login Screen


ZyXEL
ZyXEL NSA-2401
Welcome to NSA-2401
Enter Username/password and click to login.
Username:
Password:
(a maximum of 14 alphanumeric, printable characters, no single and double quotes)
Note:
Please turn on the Javascript and ActiveX control setting on Internet Explorer.
Login
Reset
© Copyright 2008 by ZyXEL Communications Corp.

You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Skip**.

Figure 6 Change Password Screen


ZyXEL
Update Admin Info
As a security precaution, it is highly recommended that you change the admin password.
New Password
Password (Confirm)
(a maximum of 14 alphanumeric, printable characters, no single and double quotes)
Apply
Ignore
© Copyright 2008 by ZyXEL Communications Corp.

The Web Configurator session automatically times out after 15 minutes. Simply log back into the NSA if this happens to you.

2.4 User-level Screens Overview

All users (including the administrator) first see the user-level access **My NSA** screen after login.

Figure 7 My NSA

The icons and language label at the top-right of the screen are visible from most screens. Use the tabs at the top of the screen to navigate between the user-level screens and menus. The following table describes the 'global' icons and tabs in the user-level screens.

Table 3 User-level Global Labels and Icons

LABEL/ICON	DESCRIPTION
Language	Select the Web Configurator language from the drop-down list box.
Help	Click the **Help** icon to open a web help page specific to the screen you are currently configuring.
Logout	Click the **Logout** icon at any time to exit the Web Configurator.
My NSA	Click this tab to go to screens where you can manage your shares and access the files on public shares. The administrator must go into the administration screens to manage other user's shares.
Password	Click this tab to go to a screen where you can change your password.
Administration	This tab displays when you log in as the administrator. Click the tab to go to screens where you can manage advanced configurations.

2.5 My NSA Screen

Use the **My NSA** screens to manage your shares and access the files in folders to which you have access.

A share is a set of user access permissions for a specific folder on a volume (gives someone access to a folder). It is similar to a shared folder in Windows, but the access rights are independent of the folder (you configure the share and the folder separately). You can map a share to a network drive for easy and familiar file transfer for Windows users.

The main **My NSA** screen displays the shares to which you have access.

Figure 8 My NSA Screen

The following table describes this screen.

Table 4 My NSA Screen

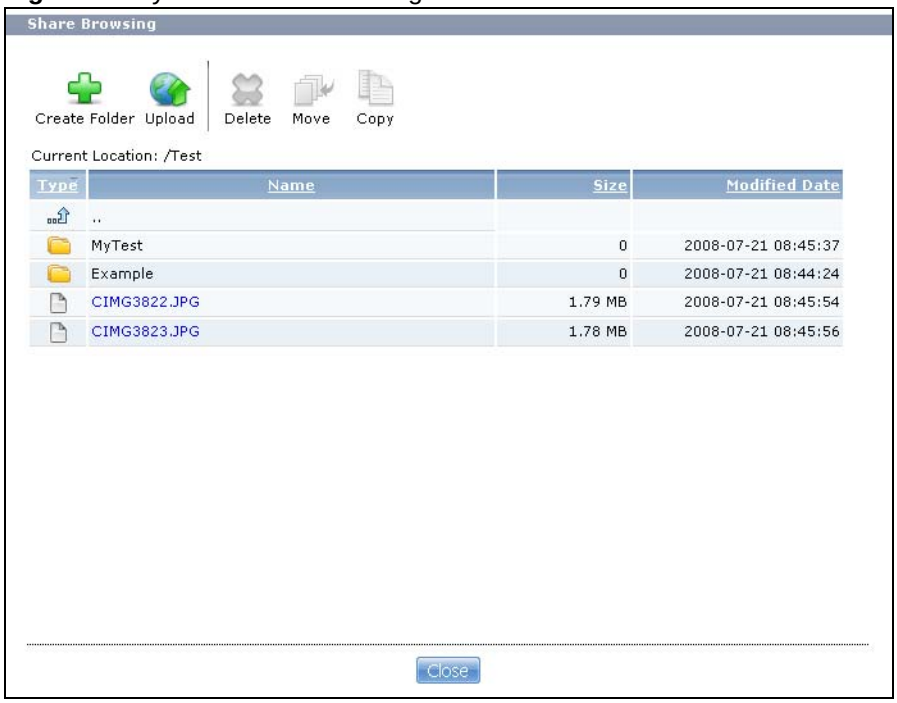
LABEL	DESCRIPTION
My Own Shares	These are the shares that you own (and manage). The share icons are folder shaped. Click a share icon to access the share's contents. **System Share** This icon displays for a system share created by the NSA. **User-created Share** This icon displays for a user-created share. **External (USB) Share** This icon displays for a share on an external (USB) device. An external share's icon disappears if the share is not currently available (because the USB device was removed for example). The administrator owns and manages the public shares.
Configure	Click this button to see and configure the management details for a share.
Other Shares	These are other shares on the internal hard drives or external (USB) devices that you can access (but not manage).

2.5.1 My NSA Share Browsing Screen

Click **My NSA** and then click a share to open the following screen. Use the **My NSA** share browsing screens to see and access share contents.

- Click a folder's name to go into the folder.
- Click a file's name to be able to save the file to your computer.
- Click the play icon to play the file. At the time of writing this is only for MP3 files.
- Click to the right of a file or folder name to select it.
- Use the [SHIFT] key to select a range of entries. Hold down the [CTRL] key to select multiple individual entries.

Figure 9 My NSA Share Browsing



The following table describes the icons in this screen.

Table 5 My NSA Share Browsing Icons

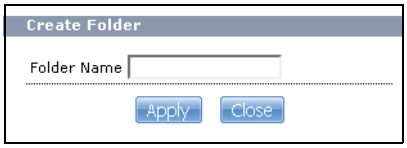
ICON	DESCRIPTION
	Create Folder Click this icon to open a screen where you can create a new folder. 
	Upload Click this button to copy a file from your computer to this location in the NSA.

Table 5 My NSA Share Browsing Icons (continued)

ICON	DESCRIPTION
	Delete Select a folder(s) or file(s) and click this icon to remove the folder(s) or file(s).
	Move The administrator can select a folder or file and click this button to move it to another location within this share or another share that you can access.
	Copy The administrator can select a folder or file and click this button to move create a copy of it in another location within this share or another share that you can access.
	Sort Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.
	Up One Level Click this icon to go to the next higher layer in the share's folder tree.
	Folder Click this icon to browse the folder.
	File Click this icon to select a file.

The following table describes the labels in this screen.

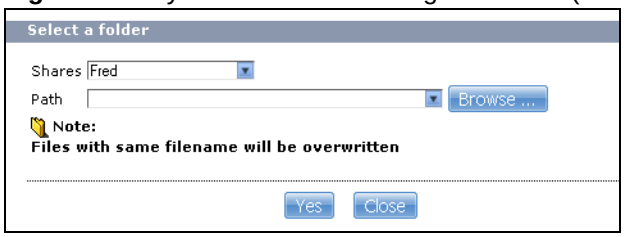
Table 6 My NSA Share Browsing

LABEL	DESCRIPTION
Current location	This is the name of the share and folder path that you are in.
Type	The icon in this column identifies the entry as a folder or a file. The folder with an arrow pointing up is the link that takes you to the next higher layer in the share's folder tree.
Name	This column identifies the names of folders and files in the share. Click a file's name to open the file or save it to your computer. Click a folder's name to display the folder's contents.
Size	This column displays a file's size.
Modified Date	This column displays the last time the file or folder was changed (in year-month-day hour:minute:second format).
Close	Click this button to return to the **My NSA** screen.

2.5.2 My NSA Share Browsing Move to or Copy to Screen

The administrator can select a folder or file in the **My NSA** share browsing screens and click the **Move to** button or the **Copy to** button to display a share browsing screen like the following. Use the share browsing screen to select the target path for moving or copying the folder or file.

Figure 10 My NSA Share Browsing > Move to (or Copy to)



The following table describes the labels in this screen.

Table 7 My NSA Share Browsing > Move to (or Copy to)

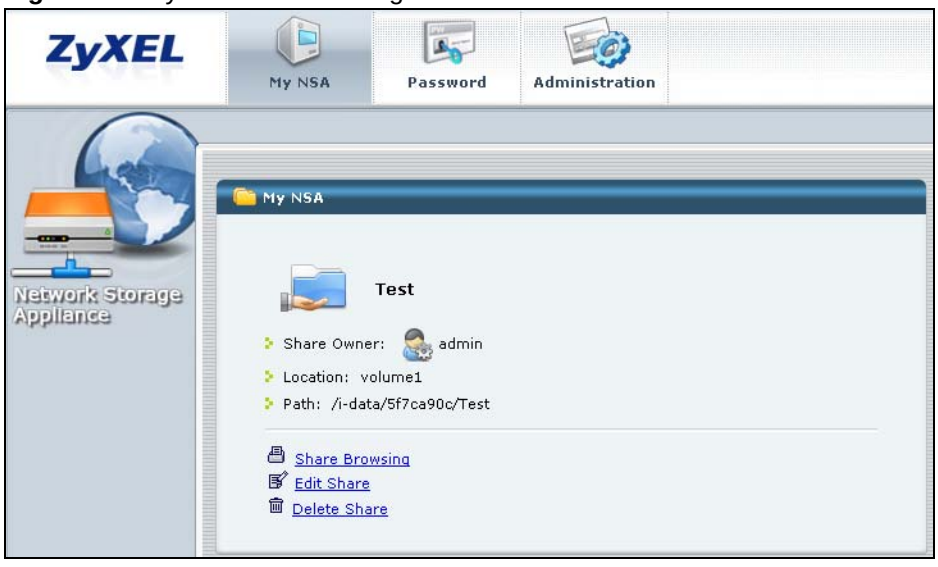
LABEL	DESCRIPTION
Shares	Select the target share.
Path	Select a folder on the NSA. You can also browse to find or create a folder on the NSA or type the location of the folder using forward slashes as branch separators.
Yes	Click this button to move or copy the file.
Close	Click this button to return to the **My NSA** share browsing screen.

2.5.3 My NSA Share Configuration

Use the **My NSA** share configuration screens to see and configure share management details.

Click **My NSA** and then the **Configure** button of one of your shares to open the following screen. This screen displays a share's management details.

Figure 11 My NSA Share Configuration



The following table describes the icons in this screen.

Table 8 My NSA Share Configuration Icons

ICON	DESCRIPTION
	Share This is the share icon followed by the name of the share.
	User This is the icon for the owner of the share.
	Share Browsing Click this icon or link to see and access the share's contents.
	Edit Share Click this icon or link to configure the share's management details.
	Delete Share Click this icon or link to remove the share and its contents.

The following table describes the labels in the this screen.

Table 9 My NSA Share Configuration

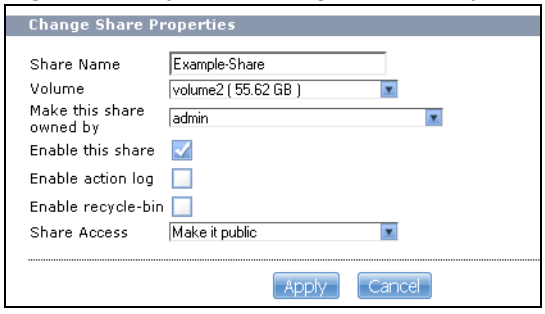
LABEL	DESCRIPTION
Share Owner	The share belongs to (and is managed by) this user account. The share owner controls access rights to the share.
Location	The share is for a folder on this volume.
Path	This is the share's file path.

2.5.4 My NSA Change Share Properties Screen

Use the **My NSA Change Share Properties** screen to configure share management details.

Click **My NSA** and a share's **Configure** button. Then click **Edt Share** to open the following screen. This screen displays a share's management details.

Figure 12 My NSA Change Share Properties



The following table describes the labels in the this screen.

Table 10 My NSA Change Share Properties

LABEL	DESCRIPTION
Share Name	Enter the name of the shared folder. The text may consist of 1 to 255 characters. See Share Name Details on page 44 for more information.
Volume	Select a volume for the share to be located on.

Table 10 My NSA Change Share Properties (continued)

LABEL	DESCRIPTION
Make this share owned by	Select an owner for the share.
Enable this share	Select this to activate the share.
Enable action log	Select this to keep a log of all actions performed on the share.
Enable recycle-bin	Select this to create a recycle bin on the share. Whenever a user with sufficient permissions deletes a file or folder, it is stored here until it is deleted permanently.
Share Access	Choose whether the share is public or private, or choose **Advanced** to open the **Share Access Configuration** screen (see Section 2.5.4.1 on page 44).
Apply	Click this to save your changes.
Cancel	Click this to discard changes and close the window.

Share Name Details

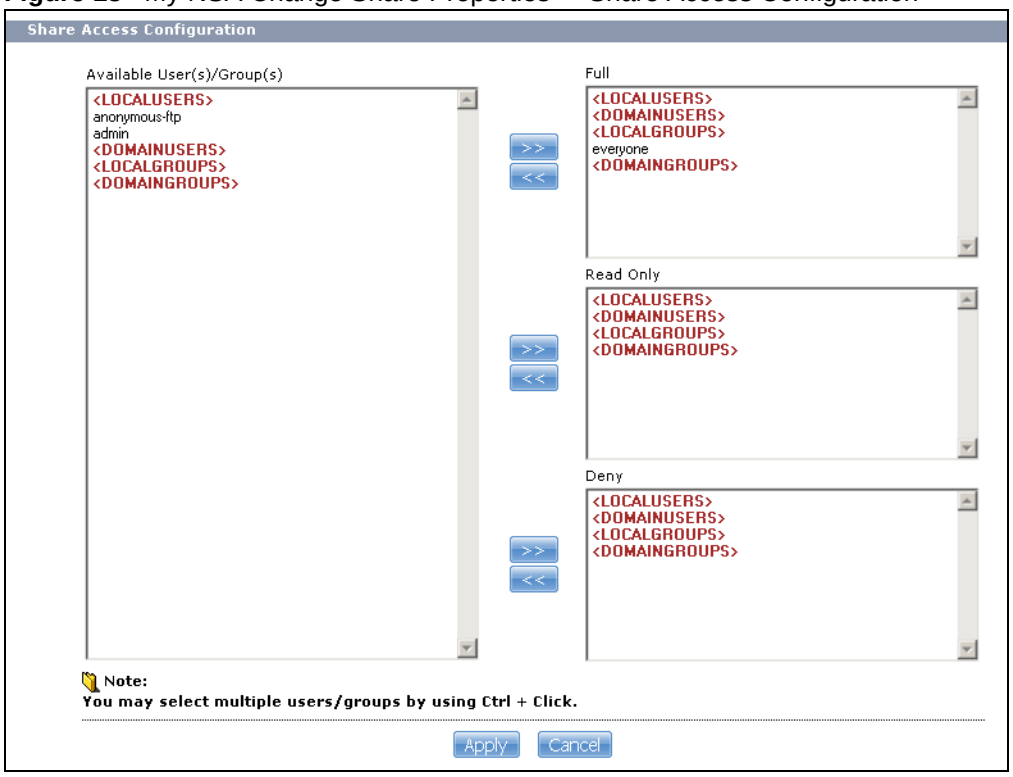
Use any character except double quotes (“), single quotes (‘), slashes (\ or /), square brackets ([ ]), colons (:), semi-colons (;), angle brackets (< >), the plus sign (+), semi-colons (;), commas (,), question marks (?), asterisks (*), and the equals sign (=).

- All leading and trailing spaces are removed automatically.
- Multiple spaces within names are converted to a single space.
- Share names must be unique (they cannot be the same as other share names).
- Share names cannot use names reserved for “automatic shares” of external USB disk volumes be unique, for example, “USB[0-9]{1,2}”, that is, a share named “USB” followed by a one or two digit number).

2.5.4.1 Share Access Configuration

This screen allows you to assign permissions to a share.

Figure 13 My NSA Change Share Properties > Share Access Configuration



The following table describes the labels in this screen.

Table 11 My NSA Change Share Properties > Share Access Configuration

LABEL	DESCRIPTION
Available Users/Groups	This displays a list of users and groups that have not yet been assigned an authority level for the share. You can assign users and groups by selecting them and clicking the right arrow.
Full Read Only Deny	Assign users and groups one of the following authority levels. **Full** - Grants read/write privileges. **Read Only** - Grants read-only privileges; files and folders cannot be modified, moved, or removed. **Deny** - Removes all privileges; files and folders cannot be read, modified, moved, or removed. You can remove users from any given authority level by selecting them and clicking the left arrow.
Apply	Click this to save your changes.
Cancel	Click this to discard changes and close the window.

2.5.5 Share and Folder Names

The name can only contain the following characters:

- Alphanumeric (A-z 0-9) and Unicode.

  The NSA allows FTP access to shares, folders or files with names encoded in the UTF-8 (8-bit UCS/Unicode Transformation Format) format. So your FTP client must support UTF-8 in order to access shares, folders or files on the NSA with Unicode names.
- Spaces
- _ [underscores]

- . [periods]
- - [dashes]

Other limitations include:

- All leading and trailing spaces are removed automatically.
- Multiple spaces within names are converted to a single space.
- Share names must be unique (they cannot be the same as other share names).
- The NSA creates automatic volume names for external (USB) disk volumes. These are a type of share, so the share name you configure cannot conflict with the external (USB) disk volume names. “ExtVol1” or “ExtVol2” are examples of external (USB) disk volume names.
- Folder names must be unique (they cannot be the same as other folder names).
- The minimum character length of a name is one character, that is a name cannot be blank.
- The maximum character length of share name is 255 characters.
- Unicode is supported for share names, although your FTP client must support UTF-8. Full support should be available in all Windows versions after Windows 2000.

2.5.6 Share Paths

A share path is the full path to a folder on a volume that will be shared, for example, /mynsa/topsecret/ugs/. This is independent from a “share name” which is the name shown for this share when accessing the share via CIFS or FTP. The path should start with a '/' (forward slash) followed by a parent folder, child folders leading to the folder that is to be shared.

2.5.7 Password Screen

Click **Password** to open the following screen. Use this screen to change an account’s password. Enter a new password and confirm it by re-entering it.

Figure 14 Password

The following table describes the labels in this screen.

Table 12 Password

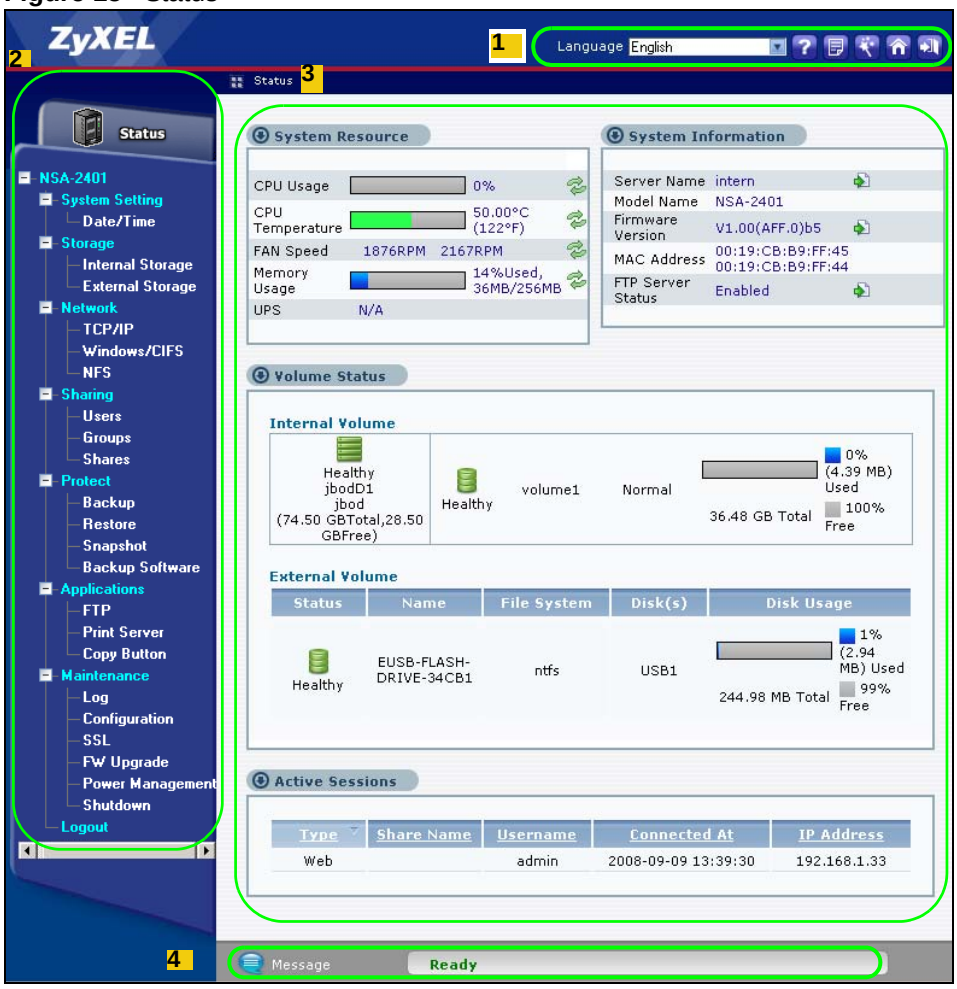
LABEL	DESCRIPTION
Account Name	Type the user name of the account for which you want to change the password.
Old Password	Type the user's current password.
New Password	Create a new password for the user. You can type from one to 14 single-byte (no Chinese characters allowed for example) ASCII characters.
Retype to confirm	You must type the exact same password that you just typed in the above field.
Apply	Click this button to save your changes back to the NSA.
Cancel	Click this button to begin configuring this screen afresh.

2.6 Administration Screens

The **Administration** tab displays when you log in as the administrator. Click **Administration** in the **My NSA** screens to open the advanced administration screens.

The first time you access the administration screens, the setup wizard opens. See the online help for details on the setup wizard screens. After you configure the setup wizard, the **Status** screen displays when you enter the advanced administration screens.

Figure 15 Status



2.6.1 Global Administration Icons

The icons and language label at the top-right of the screen (1) are visible from most of the administration screens. The following table describes the 'global' icons and labels.

Table 13 Global Labels and Icons

LABEL/ICON	DESCRIPTION
Language	Select the Web Configurator language from the drop-down list box.
	Help Click this icon to open a web help page specific to the screen you are currently configuring.
	About Click this icon to view the model name, firmware version and copyright.
	Wizards Click this icon to open a sub-menu of wizard(s).

Table 13 Global Labels and Icons

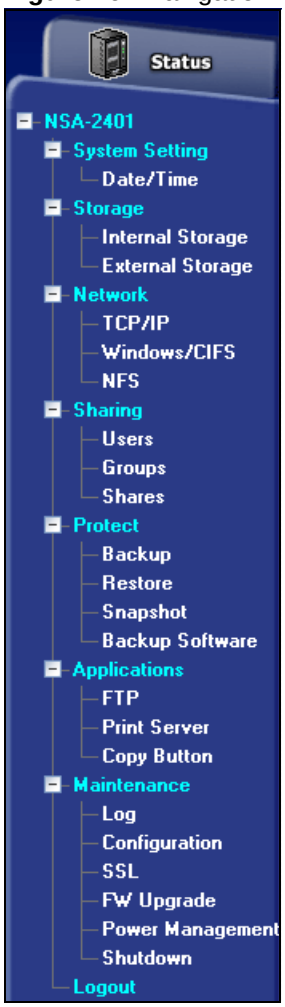
LABEL/ICON	DESCRIPTION
	Home Click this icon to return to the user-level (My NSA) screens.
	Logout Click this icon at any time to exit the Web Configurator. This is the same as clicking the **Logout** link at the bottom of the Navigation panel.

2.6.2 Navigation Panel

The navigation panel on the left of the Web Configurator screens (2) contains screen links. Click a minus (-) link to hide a category's screen links. Certain screens also contain hyper links that allow you to jump to another screen.

Click the **Status** icon to open the **Status** screen.

Figure 16 Navigation Panel Links



The following table describes the navigation panel links.

Table 14 Screens Summary

CATEGORY	SUB-LINK	FUNCTION
Status		This screen shows system information, the status of the volumes, and the users who are currently using the NSA.
System Setting	Date/Time	Choose a time zone and/or allow the NSA to synchronize with a time server.
Storage	Internal Storage	View and configure the NSA's installed disks, RAIDs, and volumes.
	External Storage	View and configure the NSA's USB-connected disks and volumes.
Network	TCP/IP	Configure the NSA's teaming mode, IP address, and DNS settings. You can also perform a ping test.
	Windows/CIFS	Specify the NSA's server name and workgroup name and choose a workgroup or domain authentication method.
	NFS	Configure NFS settings so computers with Unix or Linux operating systems can access the NSA.
Sharing	Users	Create users who may use the NSA. You may set user passwords, define storage limits per user, and associate users to a group(s).
	Groups	Create user groups and add group members.
	Shares	Create shared folders to which you can allow users and/or groups read/write access rights.
Protect	Backup	Create and manage data backups to an external USB disk drive or another NSA over the network.
	Restore	Restore a previous backup from another NSA or external USB hard drive connected to the NSA.
	Snapshot	Create and manage snapshots (records of changes to an internal volume at a particular moment in time).
	Backup Software	Use this screen to display the backup software license keys.
Applications	FTP	Enable FTP file transfer to/from the NSA, set the number of FTP connections allowed, an FTP idle timeout, and the character set.
	Print Server	View and manage the NSA's list of printers and print jobs.
	Copy Button	Configure the copy button share location.
Maintenance	Log	View the NSA system logs and configure where to send log and report emails.
	Configuration	Manage the NSA configuration file.
	SSL	Configure HTTPS and the NSA's SSL certificate.
	F/W Upgrade	Upload new firmware to your NSA.
	Power Management	Set the hard drive sleep timer.
	Shutdown	Restart your NSA or turn it off.
Logout		Click **Logout** to exit the Web Configurator. This is recommended to prevent unauthorized administrator access to the NSA.

2.6.3 Main Window

The Web Configurator's main window (3) shows the screen you select in the navigation panel. It is discussed in the rest of this document.

The **Status** screen is the first administration screen to display. See Chapter 4 on page 117 for more information about the **Status** screen.

2.6.4 Status Messages

The message text box at the bottom of the screen (4) displays status messages as you configure the NSA.

2.6.5 Common Screen Icons

The following table explains some icons that appear in several configuration screens.

Table 15 Common Configuration Screen Icons

ICON	DESCRIPTION
	wizard Click this icon to open the **Disk Setup Wizard** to create a new disk array or volume.
	Eject Select a hard drive and click this icon to shut it down. Do this before removing a hard drive to help increase its usable lifetime. Note: Ejecting a disk from a JBOD or RAID0 array causes the array to fail.
	RAID This icon represents a disk array. See the chapter on the storage screens for more details.
	Volume This icon represents a storage volume. See the chapter on the storage screens for more details.
	Disk This icon shows the status of a hard disk. See the chapter on the storage screens for more details.
	Create If you have disk space available for a new disk array, then click this icon to open a screen where you can create a new disk array.
	Delete Select an entry and click this icon to remove the entry.
	Edit Select an entry and click this icon to modify it's settings.

Table 15 Common Configuration Screen Icons (continued)

ICON	DESCRIPTION
	User This is a user icon. See the chapter on the sharing screens for details on variants of this icon.
	Share This is a share icon. See the chapter on shares for details on variants of this icon.

2.7 NSA RESET Button

Use the RESET button on the front panel of the NSA to reset either just the NSA's admin password and IP address settings or the whole factory default configuration file. Use an object such as an unfolded paper clip to press the **RESET** button.

Ideally you should back up the current NSA configuration file before resetting or reloading the factory default configuration file.

2.7.1 Reset

Do the following to only reset the administrator password and IP address settings to the defaults.

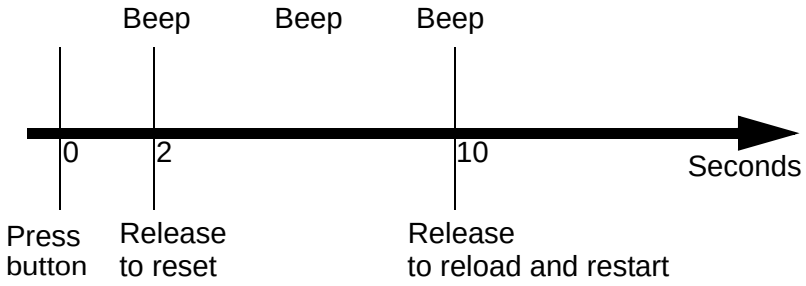
Press the **RESET** button and hold it for two seconds (you will hear one beep) and release it. The NSA sounds another single beep after you release the button as confirmation.

2.7.2 Reload Factory Default Configuration File

Do the following to reload the factory default configuration file. This resets the admin password and IP address settings to the default settings AND erases all other configurations such as user/group/share names, passwords, and share access rights.

Press the **RESET** button and hold it for ten seconds (you will hear three beeps) and release it. The NSA sounds three more beeps after you release the button as confirmation.

Figure 17 Reset and Reload Timeline



The NSA automatically restarts to complete reloading the factory default configuration file.

3

Tutorials

3.1 Overview

These tutorials show you how to perform the following common tasks:

- How to Configure Sharing: page 55
- How to Use Shares: page 61
- How to Find the NSA in OS X: page 65
- How to Configure Security: page 68
- Power Resume: page 89
- How to Use Backups and Snapshots: page 89
- How to Increase the NSA's Storage Capacity: page 106

3.2 How to Configure Sharing

This section covers how to create user accounts, groups, and shares.

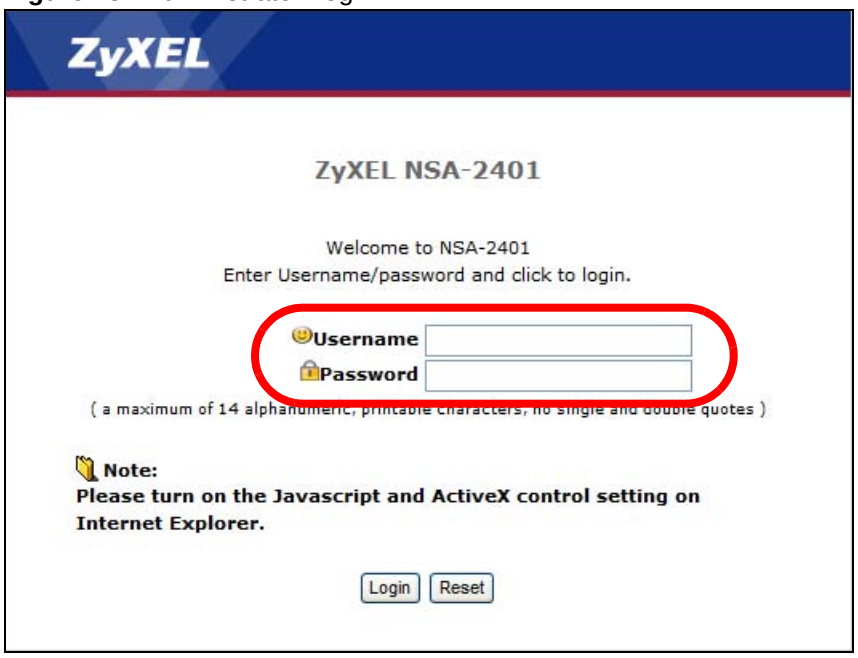
You can customize account permissions to give different users different levels of access to individual files and folders hosted on the NSA. For example, if you intend to use the NSA within a single department you may decide to give all the members of that department read and write access to all the files located on it. You could also decide to give management read and write access to some files and give other employees read-only access. Using the tools built into the ZyXEL Web Configurator, you can do just this.

3.2.1 Setting Up User Accounts

As the administrator of the NSA, one of the first tasks you will want to do is set up accounts for everyone who needs to use it. Suppose you need accounts for a vice president named Gonzo and a manager named Kermit. Do the following to create a user account.

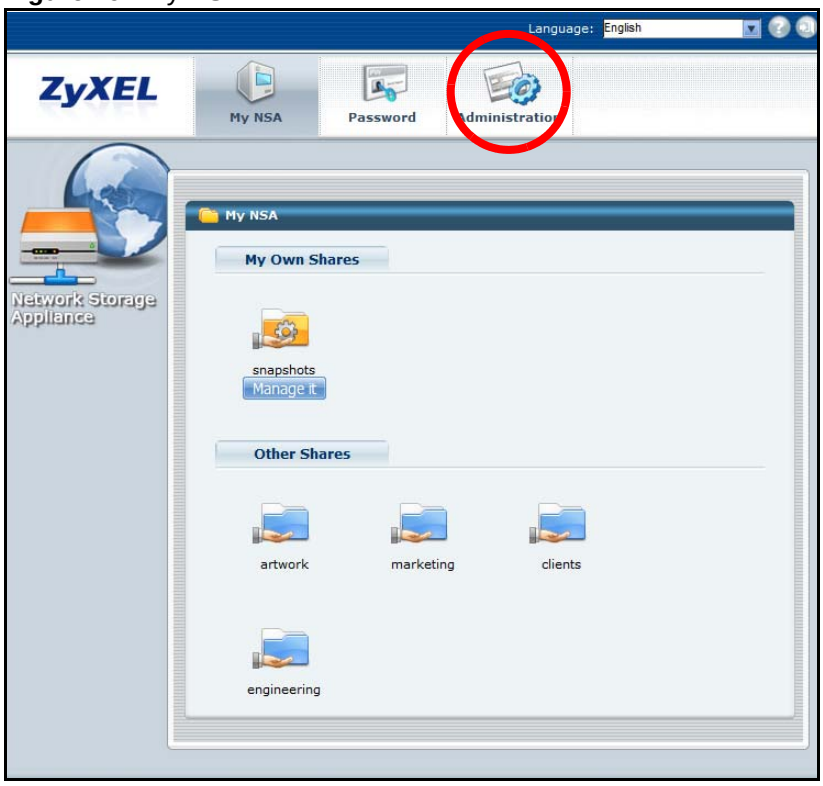
1 Log into the Web Configurator using your administrator **Username** and **Password**.

Figure 18 Administrator Login



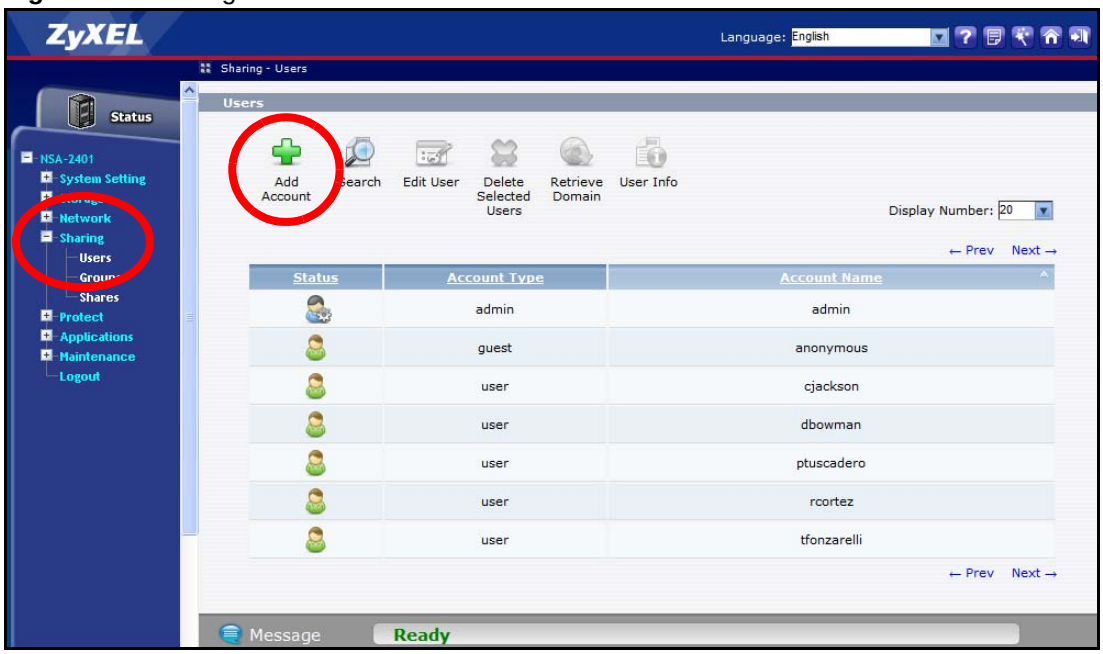
2 In the **My NSA** screen, click **Administration**.

Figure 19 My NSA



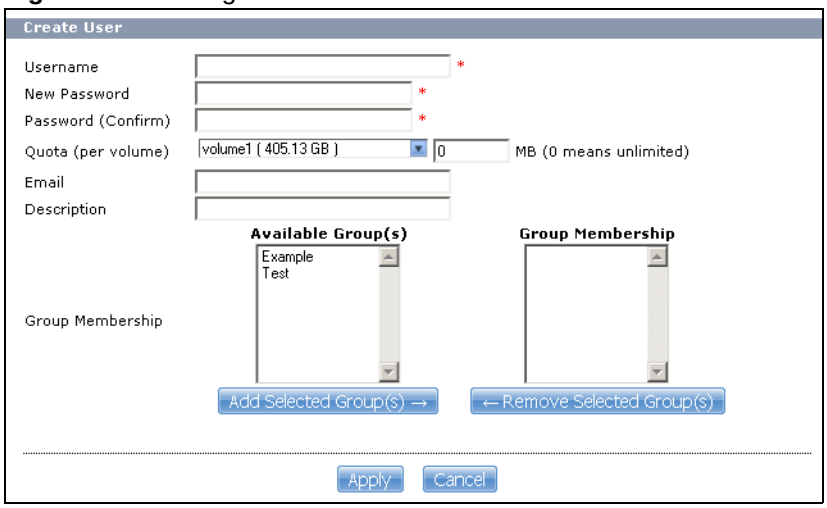
3 Once the Web Configurator workspace appears, click **Sharing** > **Users** to open the user account management area.

Figure 20 Sharing > Users



4 Click **Add Account** to open the **Create a New Account** screen.

Figure 21 Sharing > Users > Create a New Account



- Enter an account name and password.
- Set how many megabytes of storage the account can use in each of the NSA's volumes. You can set a different quota for each volume. A value of "0" MB means unlimited storage.
- Enter the user's e-mail address and any details or identifying information specific to the user account.
- Select the groups to which you want to assign this account.
- Click **Apply**.

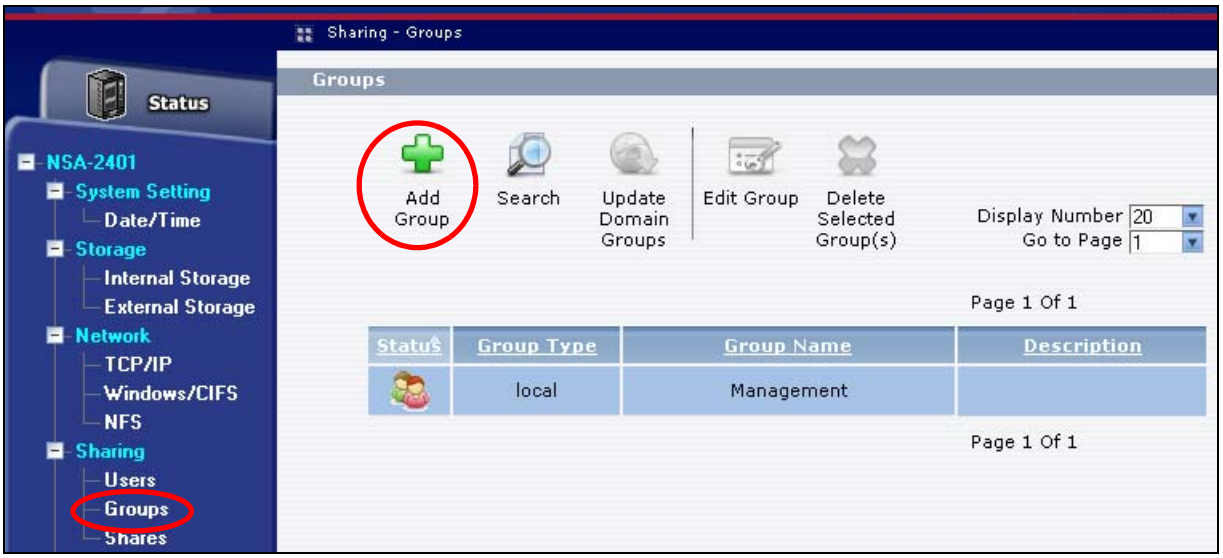
5 Repeat these steps for the other user accounts you need.

3.2.2 Setting Up Groups

After you create accounts, the next thing you'll want to do is organize the user accounts into groups. This example creates a senior management group with vice president Gonzo as a member. You can add other members later.

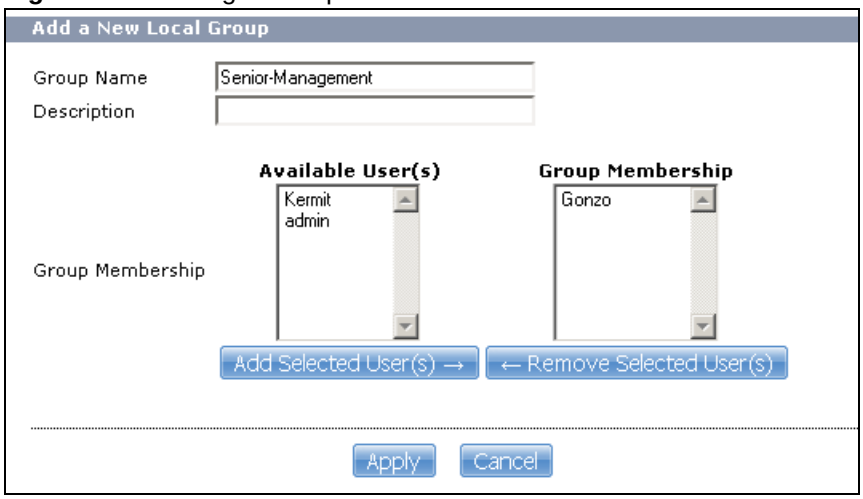
1 Click **Sharing** > **Groups** > **Add Group**.

Figure 22 Groups



2 Specify a name for the group. Select **Gonzo** and click **Add Selected User(s)** to include Gonzo in the group. Click **Apply**.

Figure 23 Sharing > Groups > Add Share



3.2.3 Setting Up Shares

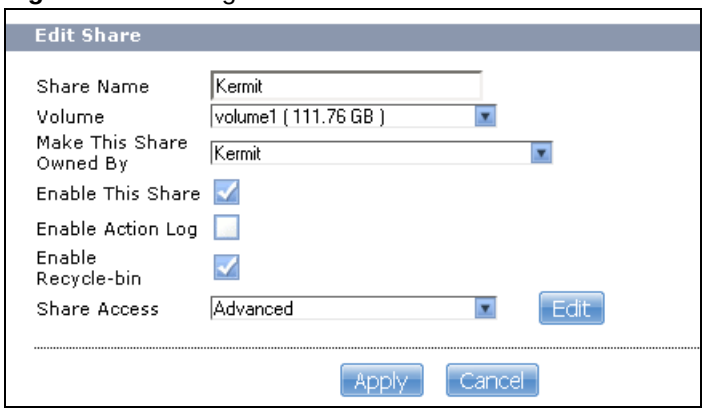
You've created accounts for Gonzo and Kermit and now you want to create a share for each of them. You also have a senior management group. You want to allow the users in the senior management group to access both shares while Kermit can access his own share.

1 Click **Sharing** > **Shares** > **Add Share**.

Figure 24 Shares

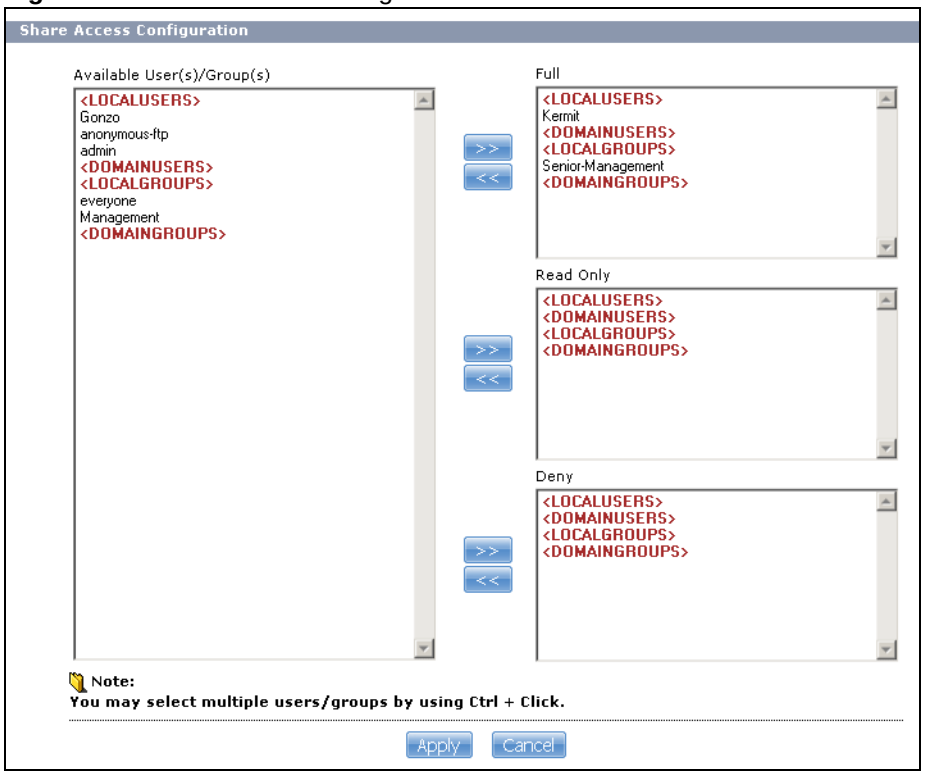
2 Specify a name for the share and select the volume it should be on. Select Kermit as the owner and set the **Share Access** to **Advanced** and click **Edit**.

Figure 25 Sharing > Shares > Add Share



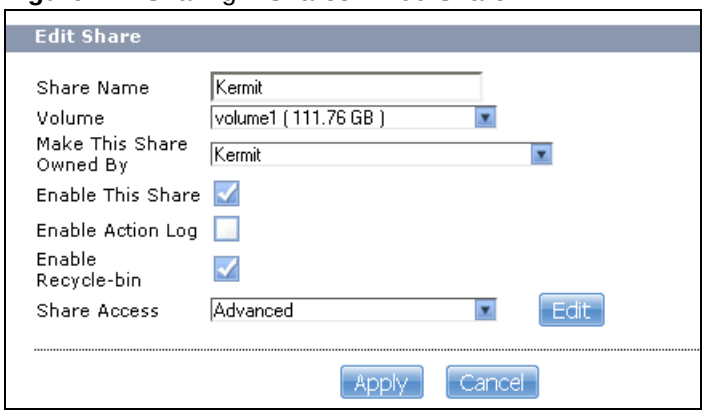
3 Include **Senior-Management** under **Full** and click **Apply**. This way both Kermit and the senior managers have full access to the share.

Figure 26 Share Access Configuration



4 Back in the **Edit Shares** screen, click **Apply**.

Figure 27 Sharing > Shares > Add Share



Now that you have created Kermit's share, you can go through the steps again to create another share for Gonzo. For Gonzo's share, set the **Share Access** to **Keep it private to owner**.

3.3 How to Use Shares

Here is how people use the shares you have created. In this example Gonzo creates a folder named "Strategy" and puts files named 2009-Plan.doc and 2010-2014-Plans.doc into it.

3.3.1 Using a Share with Windows Explorer

Gonzo wants to use his share from his computer at the office.

1 Open Windows explorer and click **Tools** > **Map Network Drive** to open the **Map Network Drive** screen.

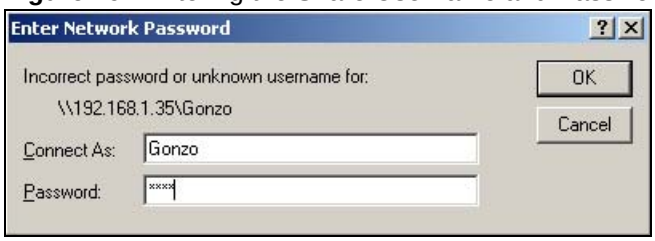
2 In the **Folder** field, enter two backslashes followed by the IP address of the NSA (192.168.1.35), another backslash, and the name of the share (Gonzo) and click **Finish**.

Figure 28 Mapping a Share

Map Network Drive
Windows can help you connect to a shared network folder and assign a drive letter to the connection so that you can access the folder using My Computer.
Specify the drive letter for the connection and the folder that you want to connect to:
Drive:
H:
Folder:
\\192.168.1.35\Gonzo
Browse...
Example: \\server\share
Reconnect at logon
Connect using a different user name.
Create a shortcut to a Web folder or FTP site.
< Back
Finish
Cancel

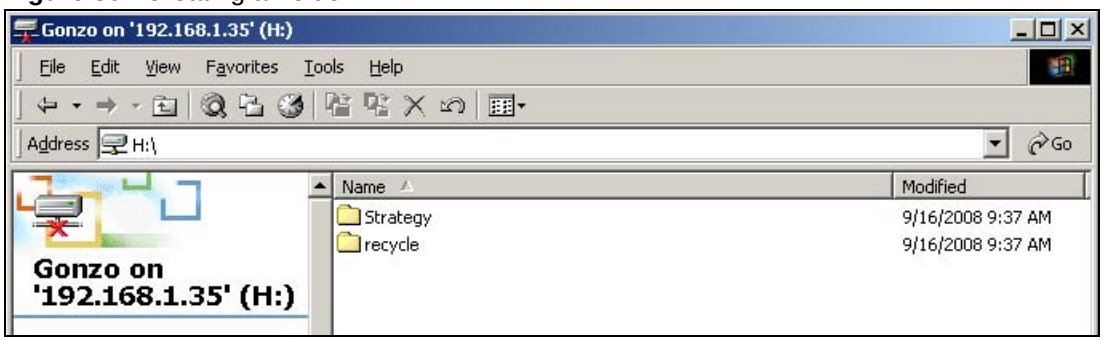
3 Enter Gonzo's username and password and click **OK**.

Figure 29 Entering the Share Username and Password



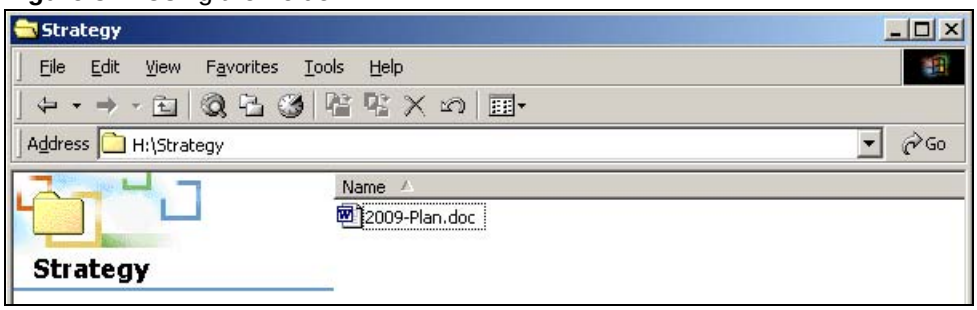
4 Now Gonzo can use the share like a drive on his computer. Click **File** > **New** > **Folder** and create a folder named "Strategy".

Figure 30 Creating a Folder



5 Copy and paste the 2009-Plan.doc file into the Strategy folder.

Figure 31 Using the Folder

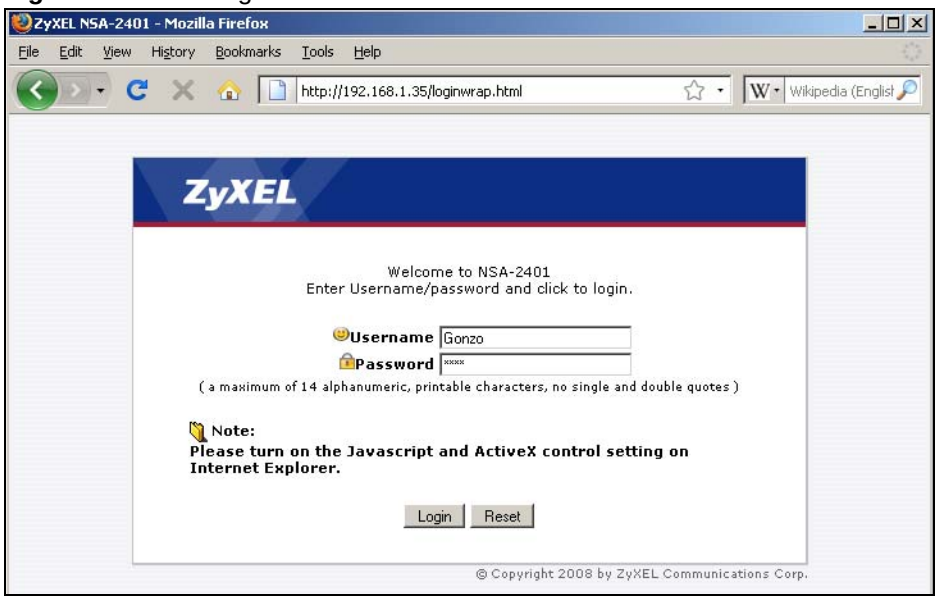


3.3.2 Using a Share with a Web Browser

Now Gonzo wants to use his web browser to add the 2010-2014-Plans.doc file to his Strategy folder.

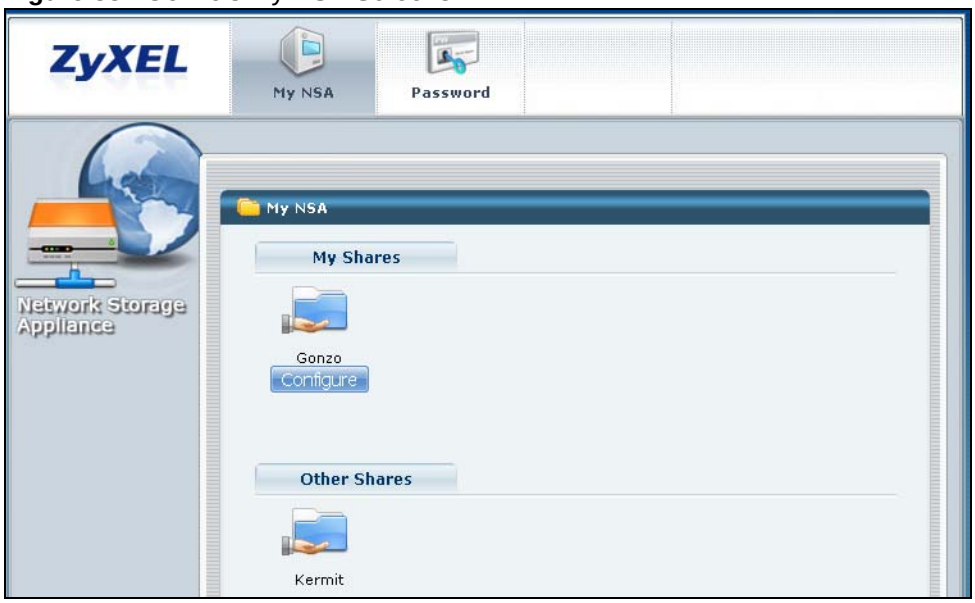
1 Open Firefox and enter http://192.168.1.35 to open the login screen. Enter Gonzo's username and password and clicks **Login**.

Figure 32 User Login


ZyXEL NSA-2401 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.35/loginwrap.html
Wikipedia (English)
ZyXEL
Welcome to NSA-2401
Enter Username/password and click to login.
Username Gonzo
Password
(a maximum of 14 alphanumeric, printable characters, no single and double quotes)
Note:
Please turn on the Javascript and ActiveX control setting on Internet Explorer.
Login Reset
© Copyright 2008 by ZyXEL Communications Corp.

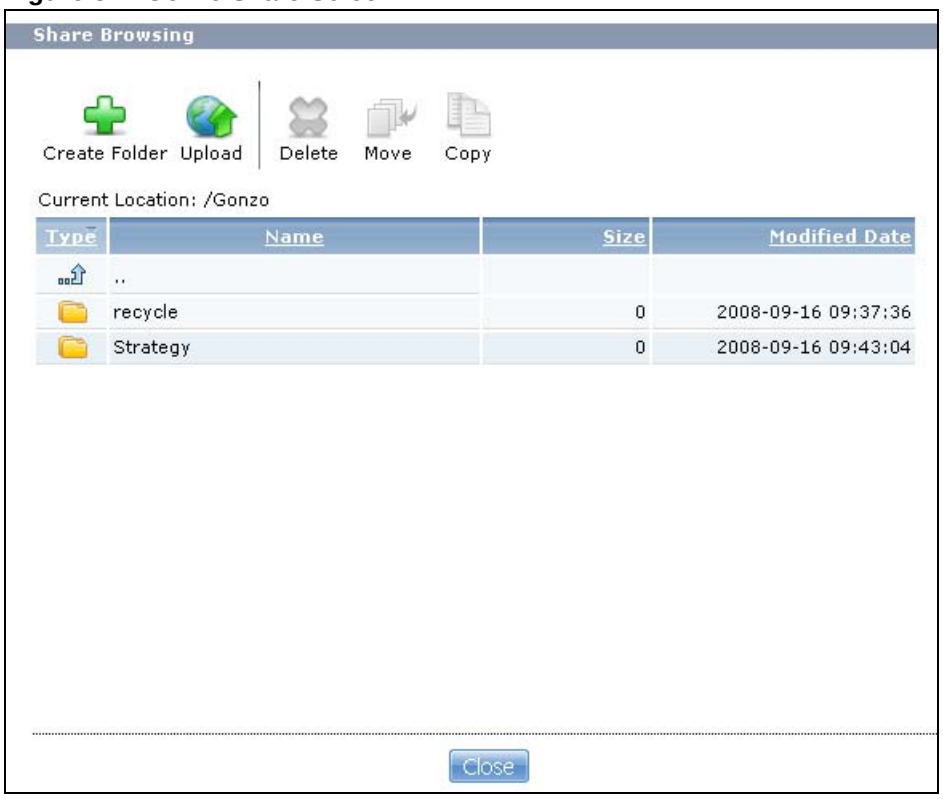
2 Click the **Gonzo** share.

Figure 33 Gonzo's My NSA Screens



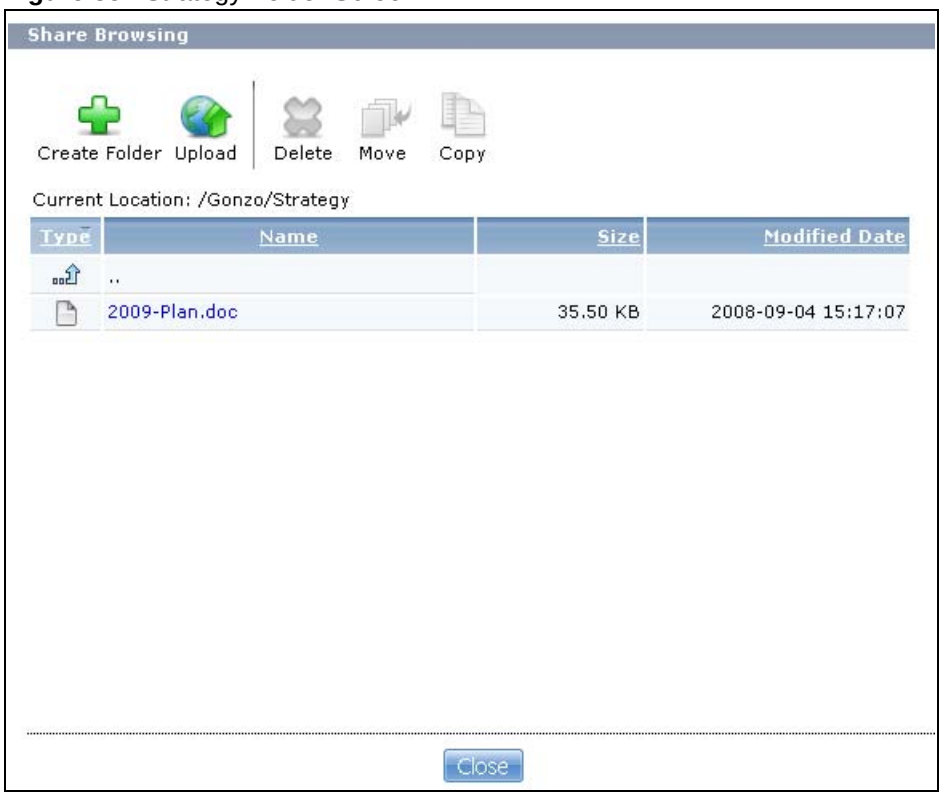
3 Open the **Strategy** share.

Figure 34 Gonzo Share Screen



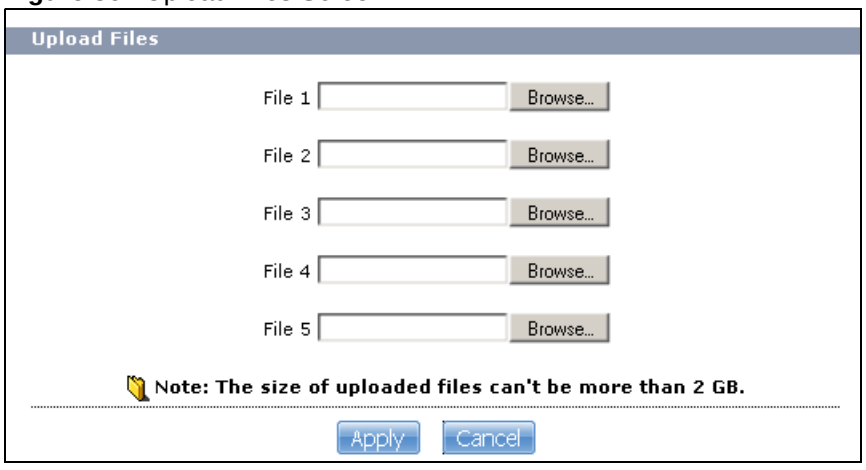
4 Click **Upload**.

Figure 35 Strategy Folder Screen



5 Browse to the 2010-2014-Plans.doc file and click **Apply**.

Figure 36 Upload Files Screen



3.4 How to Find the NSA in OS X

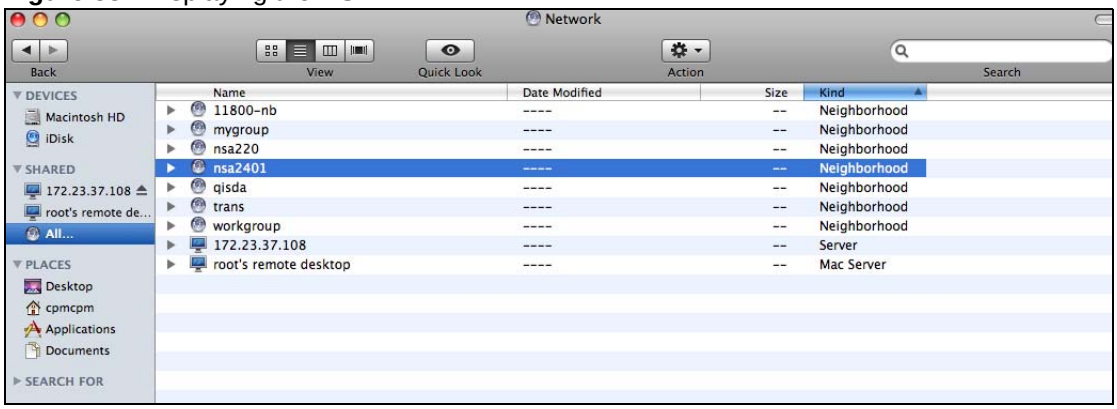
Here's how to find the NSA-2401 OS X. This example uses Mac OS X 10.5 (Leopard).

1 Click the **Finder** icon in the dock.

Figure 37 Opening the Finder

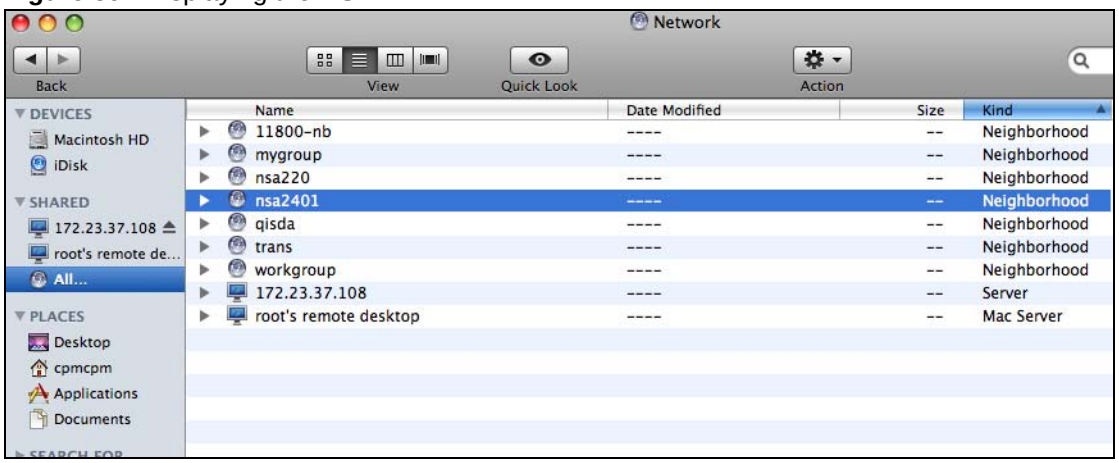
2 Select **All** under **Shared** in the sidebar. An entry for the NSA appears in the **Network** list.

Figure 38 Displaying the NSA



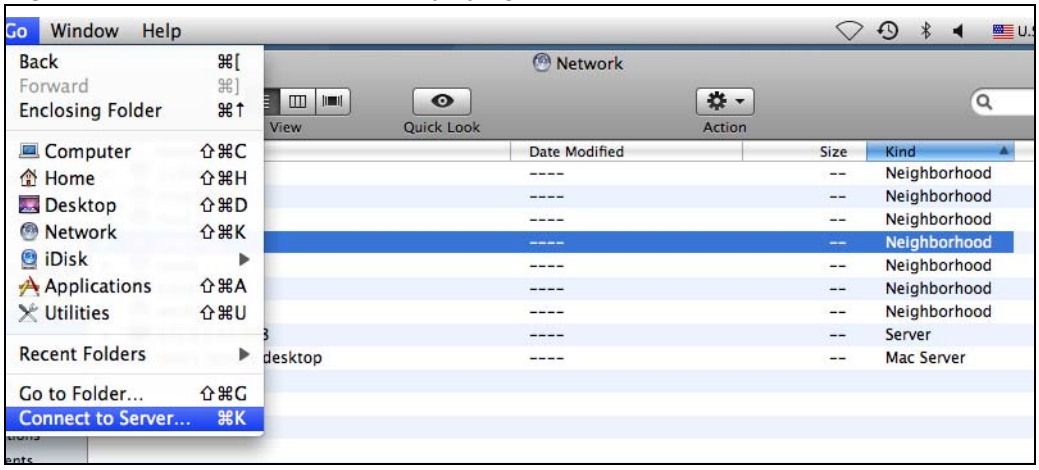
3 Click the triangle beside the NSA's name to display the shares that Gonzo can use.

Figure 39 Displaying the NSA



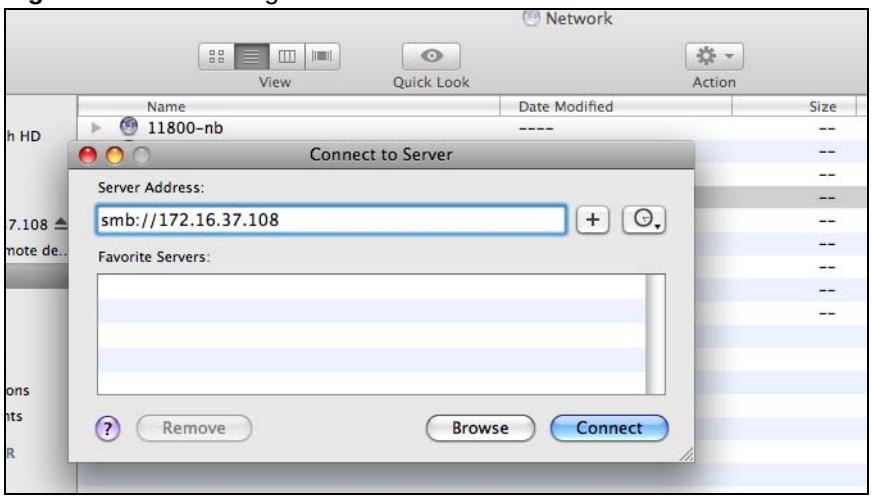
Alternatively, you can also connect directly to the NSA from the **Go Menu** in the **Finder**. Simply click **Go > Connect to Server**.

Figure 40 Alternate Method for Displaying the NSA



4 When the **Connect to Server** dialog box opens, type smb:// and the IP address of your NSA-2401 or click **Browse** to find it in your network. Click **Connect**.

Figure 41 Connecting to the NSA



5 Once connected, you can now access the NSA from the finder or directly from the desktop.

3.5 How to Configure Security

Use these tutorials to help you secure your NSA. See also Chapter 6 on page 125 for details on encrypting volumes.

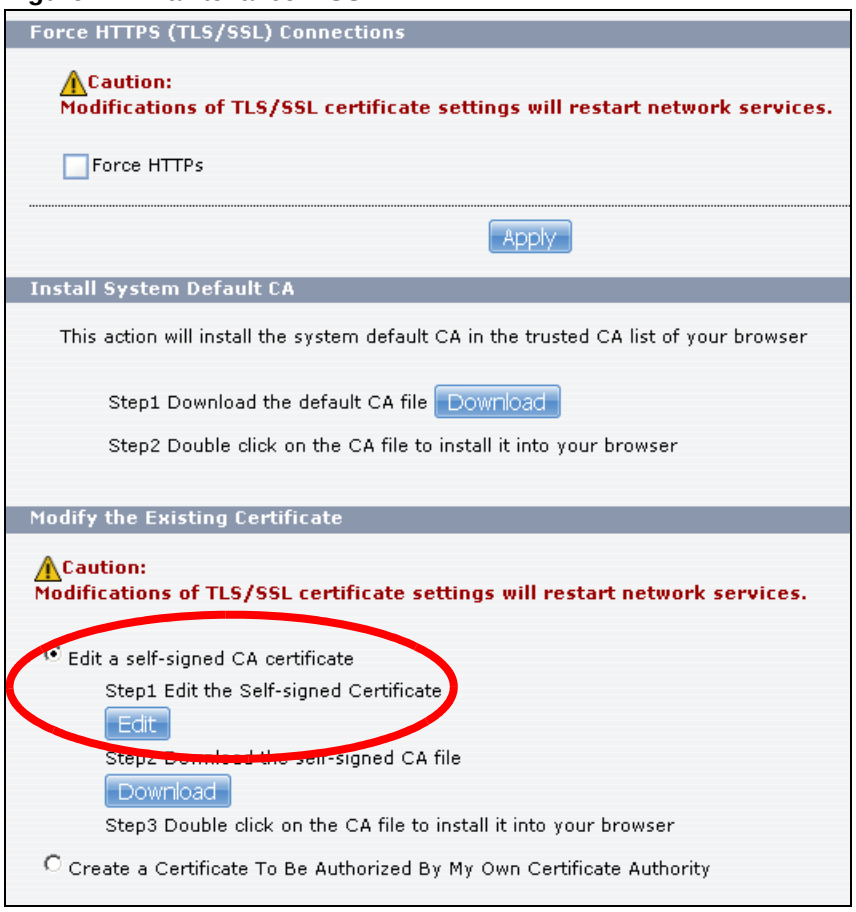
3.5.1 Configuring Security for Web Configurator Sessions

These tutorials show you how to configure security for the NSA's Web Configurator sessions. You will customize the NSA's self-signed SSL certificate and distribute it to your users.

3.5.1.1 Customizing the NSA's Certificate

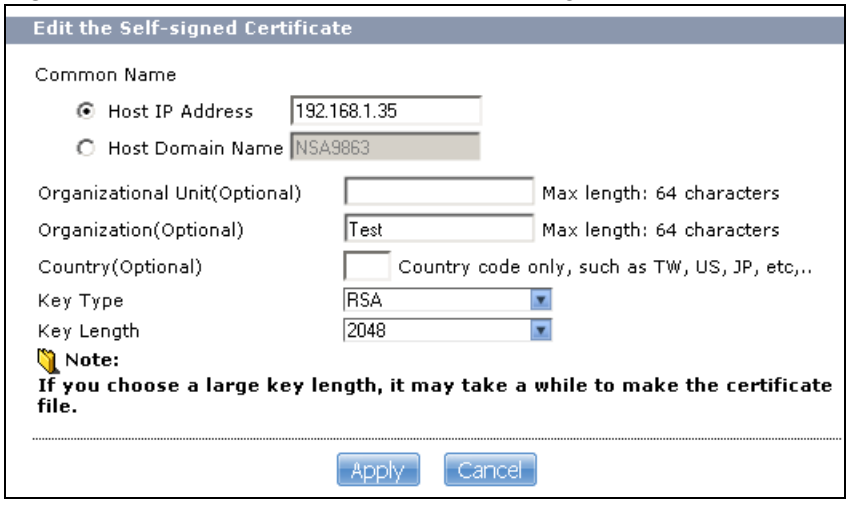
1 Click **Maintenance** > **SSL** and then select **Edit a self-signed CA certificate** and click **Edit**.

Figure 42 Maintenance > SSL


Force HTTPS (TLS/SSL) Connections
Caution:
Modifications of TLS/SSL certificate settings will restart network services.
Force HTTPs
Apply
Install System Default CA
This action will install the system default CA in the trusted CA list of your browser
Step1 Download the default CA file
Download
Step2 Double click on the CA file to install it into your browser
Modify the Existing Certificate
Caution:
Modifications of TLS/SSL certificate settings will restart network services.
Edit a self-signed CA certificate
Step1 Edit the Self-signed Certificate
Edit
Download
Step3 Double click on the CA file to install it into your browser
Create a Certificate To Be Authorized By My Own Certificate Authority

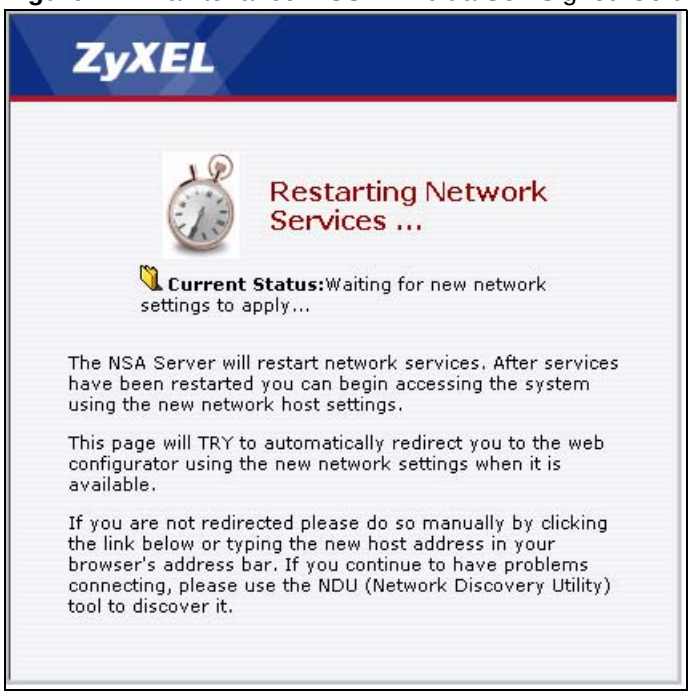
2 Next, let's modify the certificate by changing the **Common Name** to this NSA's IP address of 192.168.1.35, the **Organization** to "Test" and the **Key Length** to **2048**.

Figure 43 Maintenance > SSL > Edit a Self-Signed Certificate



3 The NSA restarts its network services and returns you to the login screen.

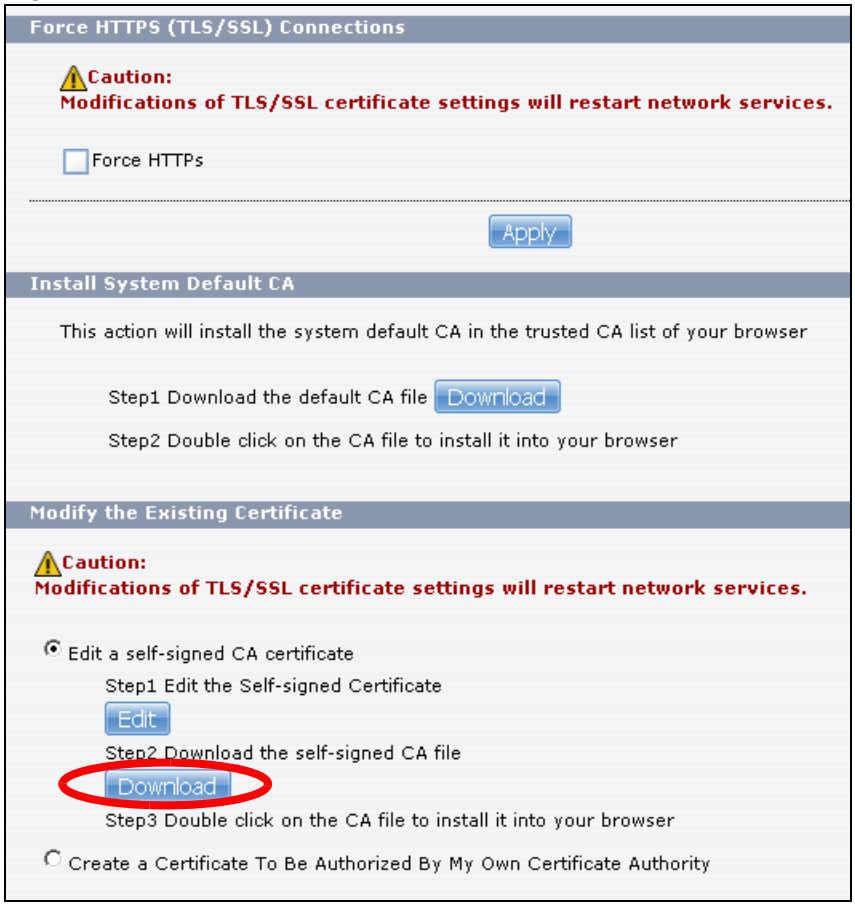
Figure 44 Maintenance > SSL > Edit a Self-Signed Certificate


ZyXEL
Restarting Network Services ...
Current Status:Waiting for new network settings to apply...
The NSA Server will restart network services. After services have been restarted you can begin accessing the system using the new network host settings.
This page will TRY to automatically redirect you to the web configurator using the new network settings when it is available.
If you are not redirected please do so manually by clicking the link below or typing the new host address in your browser's address bar. If you continue to have problems connecting, please use the NDU (Network Discovery Utility) tool to discover it.

3.5.1.2 Downloading and Installing the NSA's Customized Certificate

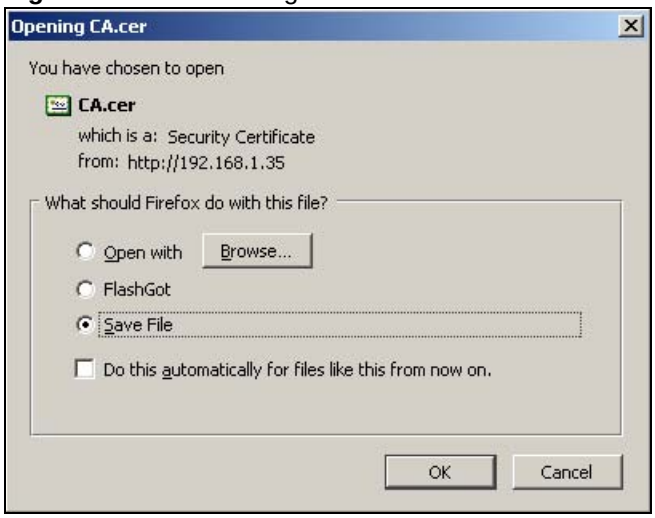
1 Log in and return to **Maintenance** > **SSL**. Under **Modify the Existing Certificate**, click **Download**.

Figure 45 Maintenance > SSL


Force HTTPS (TLS/SSL) Connections
Caution:
Modifications of TLS/SSL certificate settings will restart network services.
Force HTTPs
Apply
Install System Default CA
This action will install the system default CA in the trusted CA list of your browser
Step1 Download the default CA file
Download
Step2 Double click on the CA file to install it into your browser
Modify the Existing Certificate
Caution:
Modifications of TLS/SSL certificate settings will restart network services.
Edit a self-signed CA certificate
Step1 Edit the Self-signed Certificate
Edit
Step2 Download the self-signed CA file
Download
Step3 Double click on the CA file to install it into your browser
Create a Certificate To Be Authorized By My Own Certificate Authority

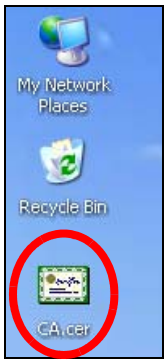
2 Save the file to your computer.

Figure 46 Downloading the NSA's Certificate



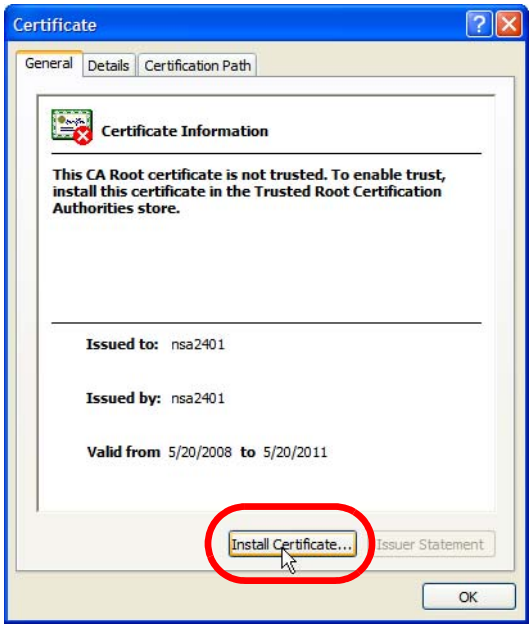
3 Find the certificate file on your computer and double-click it.

Figure 47 Downloading the NSA's Certificate



4 Install the certificate. The rest of the steps in this section are an example of installing a certificate in Windows. See Appendix C on page 299 for other examples. In the **Certificate** dialog box, click **Install Certificate**.

Figure 48 Certificate



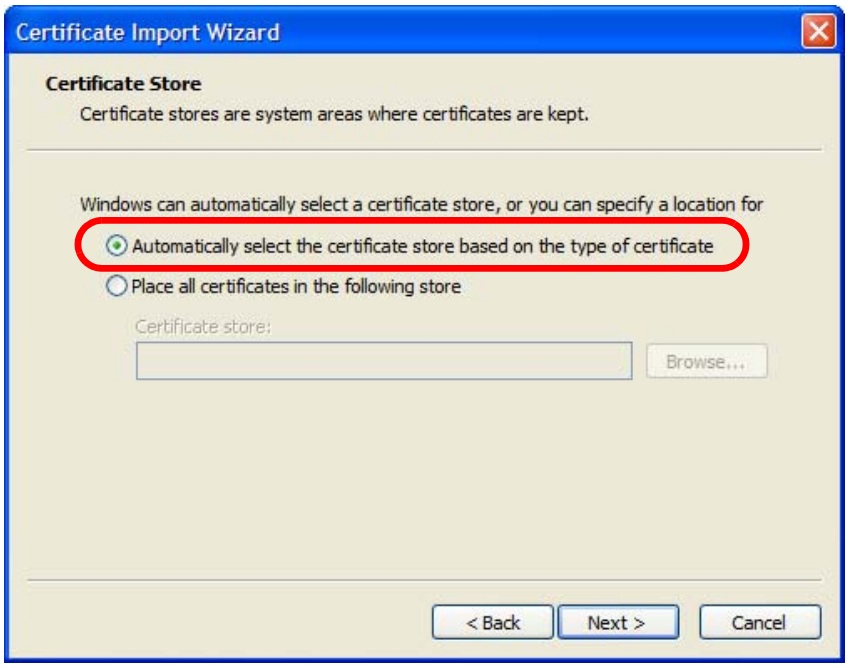
5 In the **Certificate Import Wizard**, click **Next**.

Figure 49 Certificate Import Wizard: Welcome

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

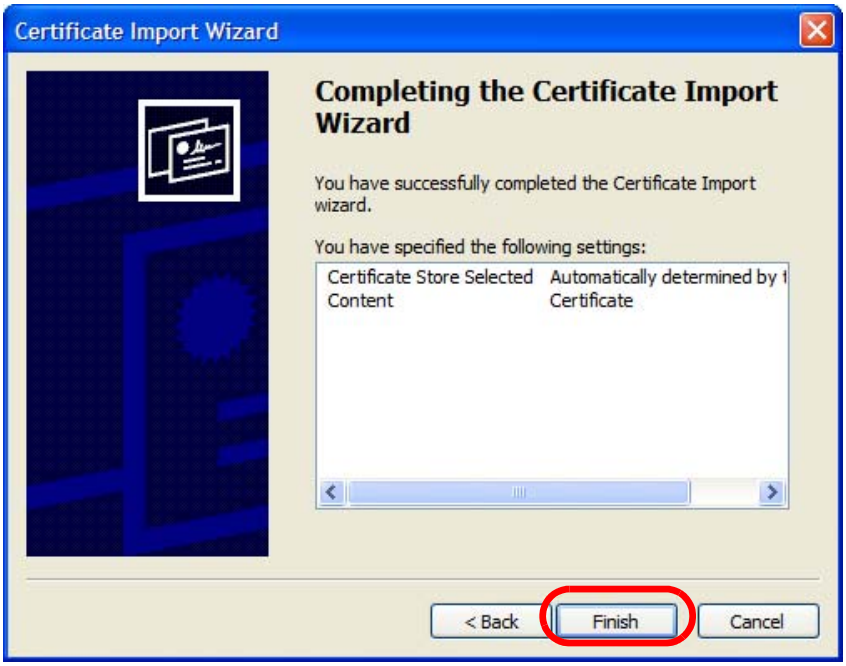
6 Leave **Automatically select certificate store based on the type of certificate** selected and click **Next**.

Figure 50 Certificate Import Wizard: Certificate Store


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel

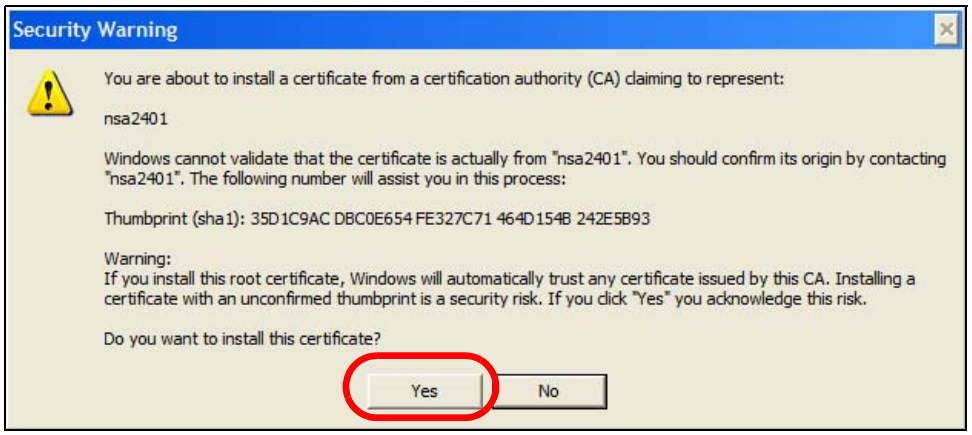
7 In the **Completing the Certificate Import Wizard** screen, click **Finish**.

Figure 51 Certificate Import Wizard: Finish



8 If you are presented with another **Security Warning**, click **Yes**.

Figure 52 Security Warning


Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
nsa2401
Windows cannot validate that the certificate is actually from "nsa2401". You should confirm its origin by contacting "nsa2401". The following number will assist you in this process:
Thumbprint (sha1): 35D1C9AC DBC0E654 FE327C71 464D154B 242E5B93
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No

9 Finally, click **OK** when presented with the successful certificate installation message.

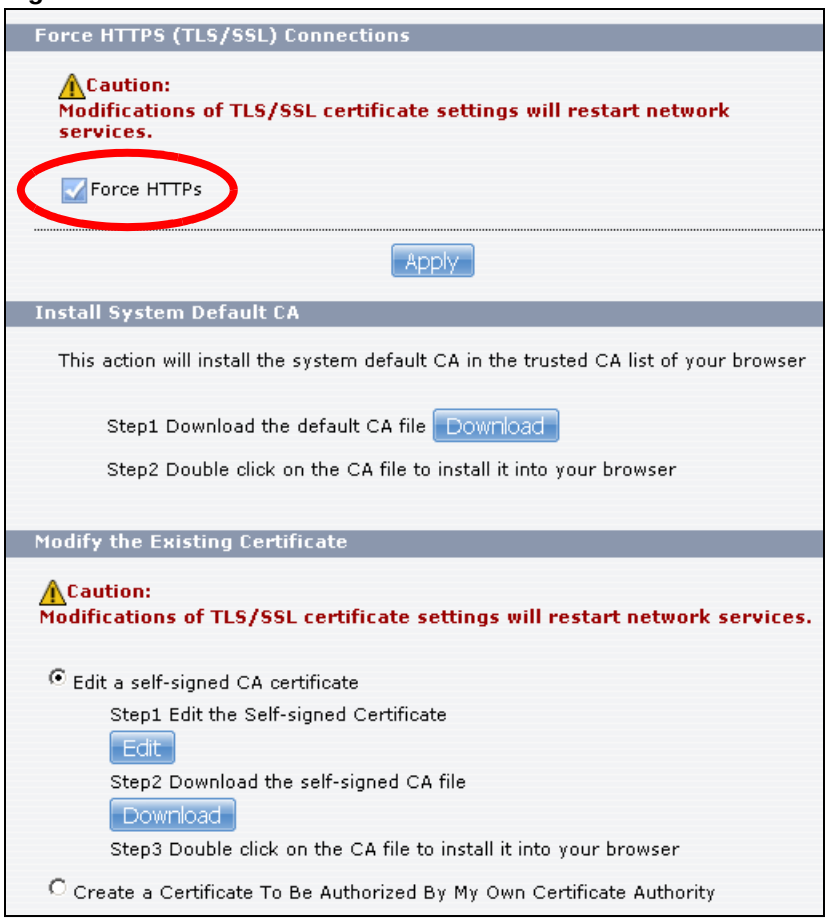
Figure 53 Certificate Import Wizard: Successful

3.5.1.3 Turn on the NSA's Web Security

Now that you have customized the NSA's certificate and installed it in your computer, you can turn on security for your Web Configurator sessions. This example uses Firefox 3.0. See Appendix C on page 299 for more information on browsers and certificates.

1 Close your web browser and open it again to reset its session with the NSA. Log in and click **Maintenance** > **SSL**. Select **Force HTTPS** and click **Apply**.

Figure 54 Maintenance > SSL


Force HTTPS (TLS/SSL) Connections
Caution:
Modifications of TLS/SSL certificate settings will restart network services.
Force HTTPs
Apply
Install System Default CA
This action will install the system default CA in the trusted CA list of your browser
Step1 Download the default CA file
Download
Step2 Double click on the CA file to install it into your browser
Modify the Existing Certificate
Caution:
Modifications of TLS/SSL certificate settings will restart network services.
Edit a self-signed CA certificate
Step1 Edit the Self-signed Certificate
Edit
Step2 Download the self-signed CA file
Download
Step3 Double click on the CA file to install it into your browser
Create a Certificate To Be Authorized By My Own Certificate Authority

2 A warning screen pops up if applying your change may disconnect some users. Click **Apply** to continue.

Figure 55 Maintenance > SSL > Force HTTPS Warning

3 The NSA logs you out and automatically redirects your formerly non-secure (HTTP) connection to a secure (HTTPS) connection. Your browser may give you a warning about the device's public key certificate. Add an exception to allow your browser to bypass the warning.

Figure 56 Firefox: Secure Connection Failed

Secure Connection Failed
192.168.1.35 uses an invalid security certificate.
The certificate is not trusted because it is self signed.
The certificate is only valid for nsa2401
(Error code: sec_error_untrusted_issuer)
This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.
Or you can add an exception...

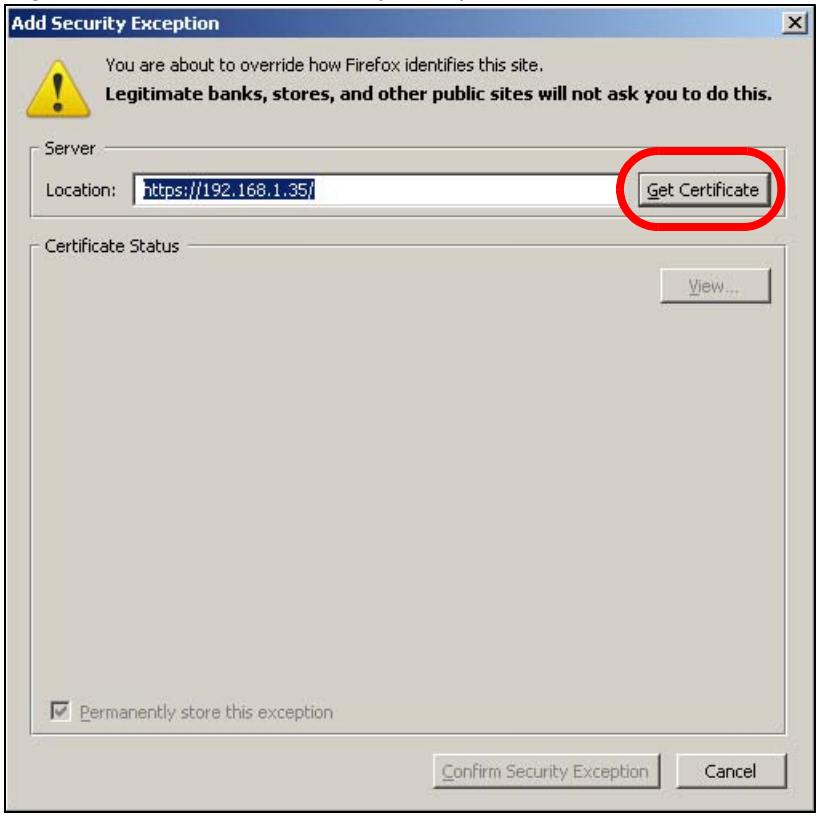
4 Click **Add Exception**.

Figure 57 Firefox: Secure Connection Failed

Secure Connection Failed
192.168.1.35 uses an invalid security certificate.
The certificate is not trusted because it is self signed.
The certificate is only valid for nsa2401
(Error code: sec_error_untrusted_issuer)
This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.
You should not add an exception if you are using an internet connection that you do not trust completely or if you are not used to seeing a warning for this server.
Get me out of here!
Add Exception...

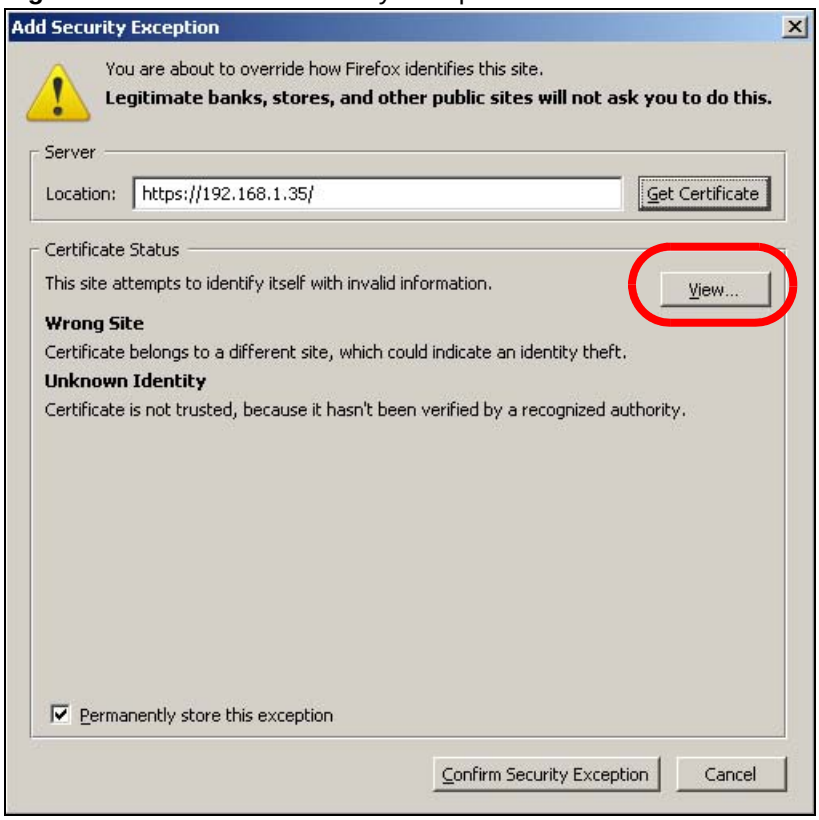
5 Click **Get Certificate**.

Figure 58 Firefox: Add Security Exception



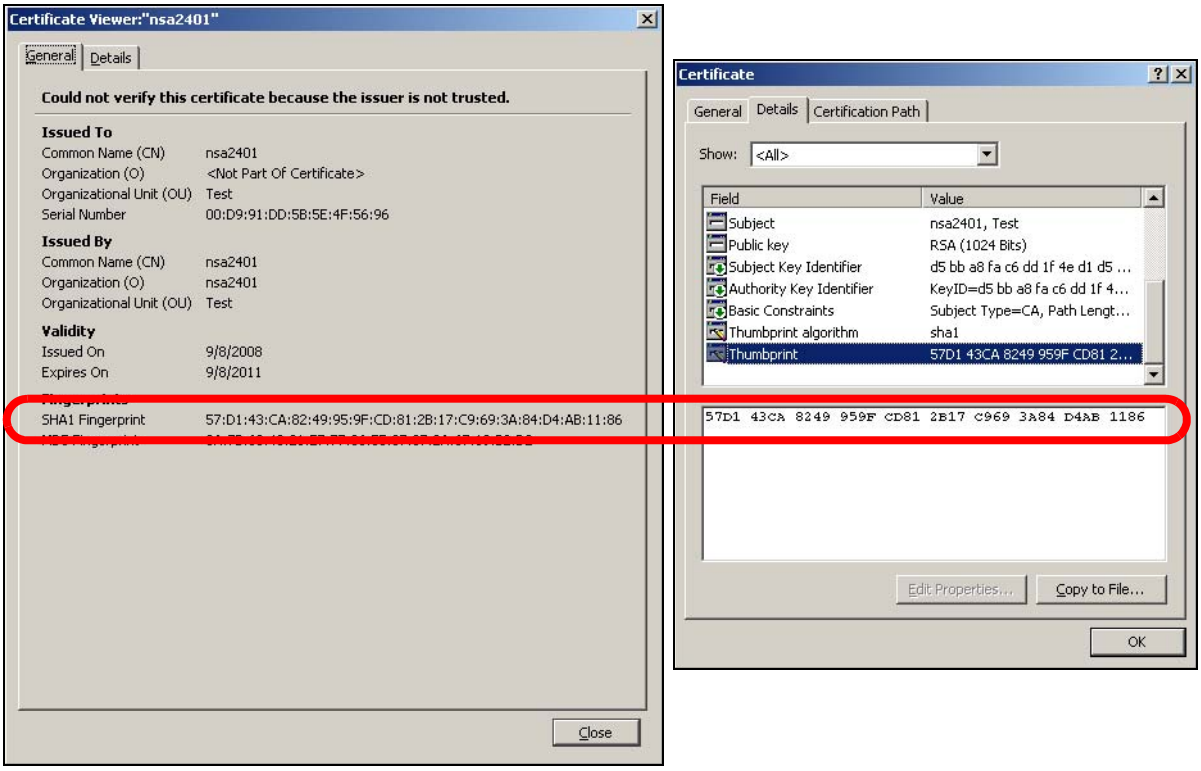
6 Before you add an exception, verify that the device to which you are trying to connect is providing the correct certificate. Click **View**.

Figure 59 Firefox: Add Security Exception


Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location:
https://192.168.1.35/
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View...
Wrong Site
Certificate belongs to a different site, which could indicate an identity theft.
Unknown Identity
Certificate is not trusted, because it hasn't been verified by a recognized authority.
Permanently store this exception
Confirm Security Exception
Cancel

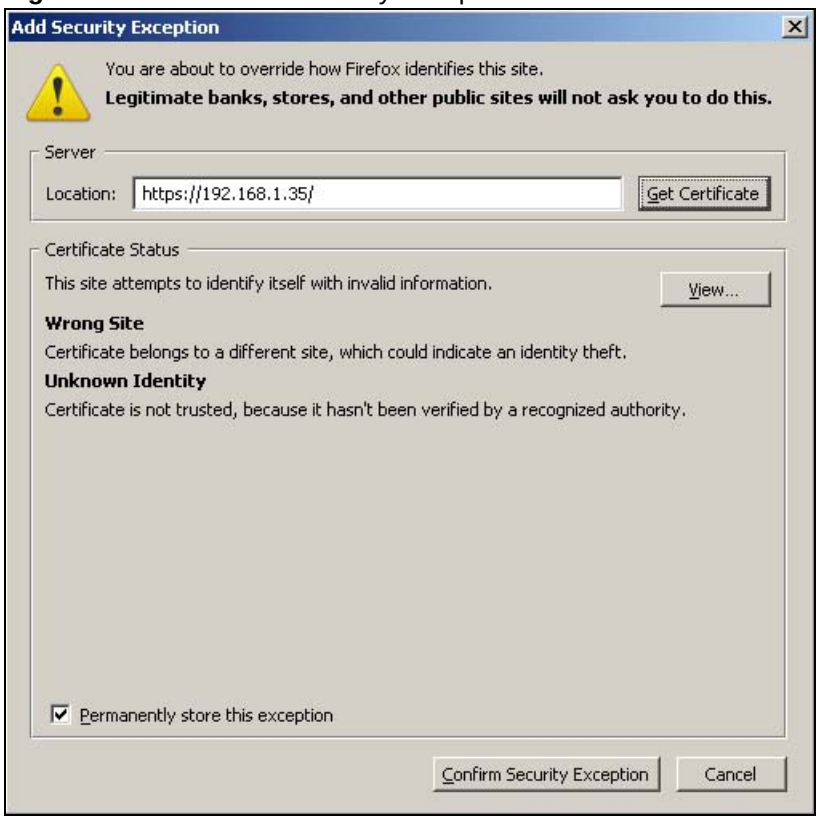
7 The SHA1 fingerprint must match the NSA's certificate you downloaded from the NSA to your computer. (Double-click the NSA's certificate file and then click **Details** and look at the **Thumbprint**). Click **Close**.

Figure 60 Firefox: Add Security Exception



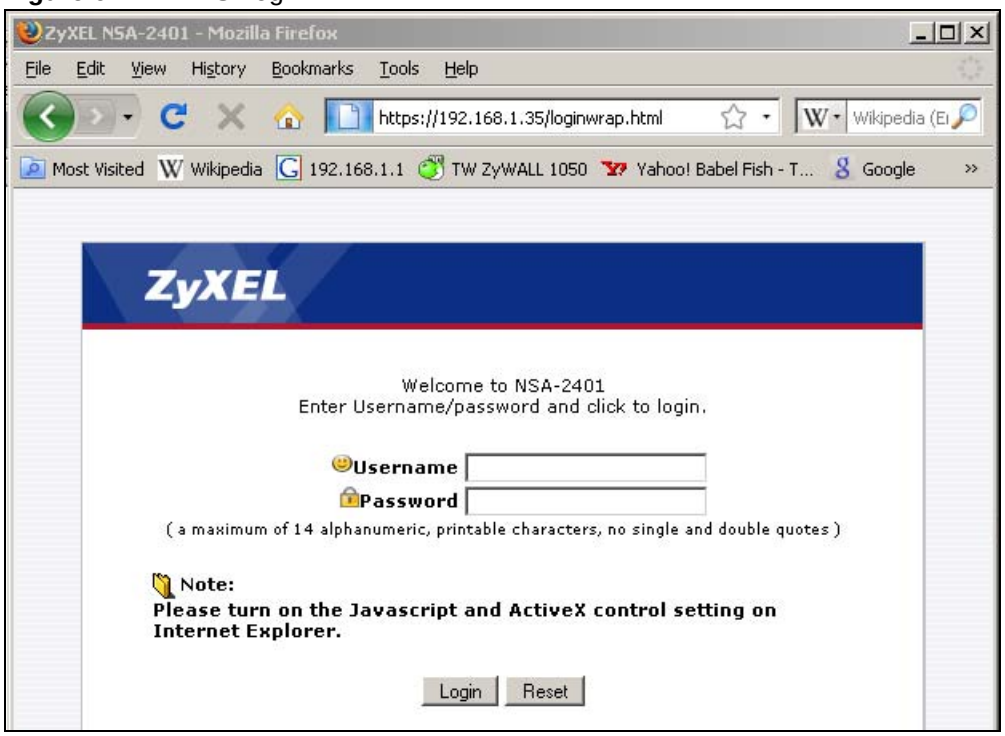
8 If the certificate fingerprints match, click **Confirm Security Exception**, otherwise click **Cancel**.

Figure 61 Firefox: Add Security Exception


Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location:
https://192.168.1.35/
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View...
Wrong Site
Certificate belongs to a different site, which could indicate an identity theft.
Unknown Identity
Certificate is not trusted, because it hasn't been verified by a recognized authority.
Permanently store this exception
Confirm Security Exception
Cancel

9 The login screen displays.

Figure 62 HTTPS Login


ZyXEL NSA-2401 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://192.168.1.35/loginwrap.html
Most Visited Wikipedia 192.168.1.1 TW ZyWALL 1050 Yahoo! Babel Fish - T... Google
ZyXEL
Welcome to NSA-2401
Enter Username/password and click to login.
Username
Password
(a maximum of 14 alphanumeric, printable characters, no single and double quotes)
Note:
Please turn on the Javascript and ActiveX control setting on Internet Explorer.
Login
Reset

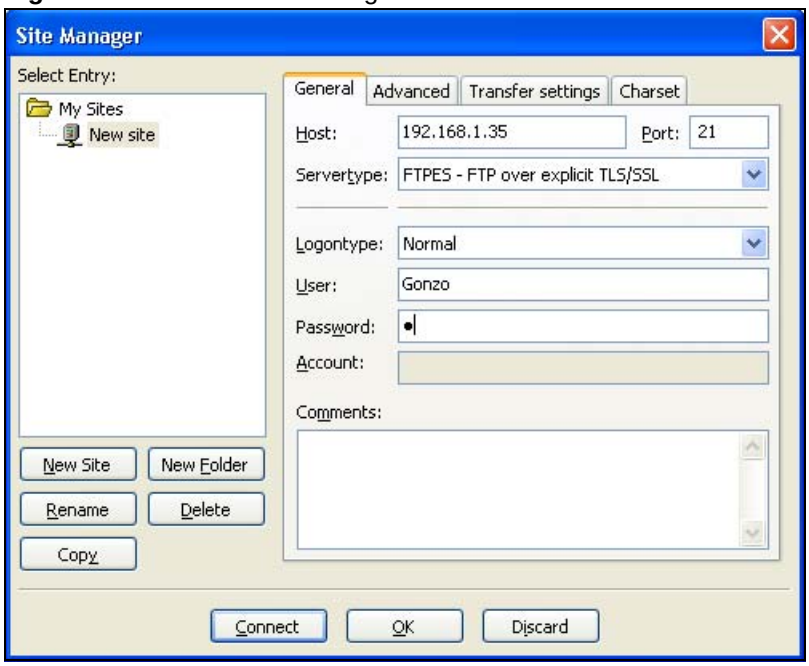
Now, anyone who connects to the NSA's Web Configurator screens will automatically do so by HTTPs. Use a secure method to let your users know the correct fingerprint for the NSA's certificate so they can check it before adding a security exception (as in steps 6 to 7 on pages 78 to 79). See the next section for how to use FTPES with the NSA for secure FTP transfers.

3.5.2 Using FTPES to Connect to the NSA

This section covers how to use FTP over Explicit TLS with the NSA for secure FTP transfers. Before you go through this section, read Section 3.5.1 on page 68 to configure HTTPS. This example uses FileZilla.

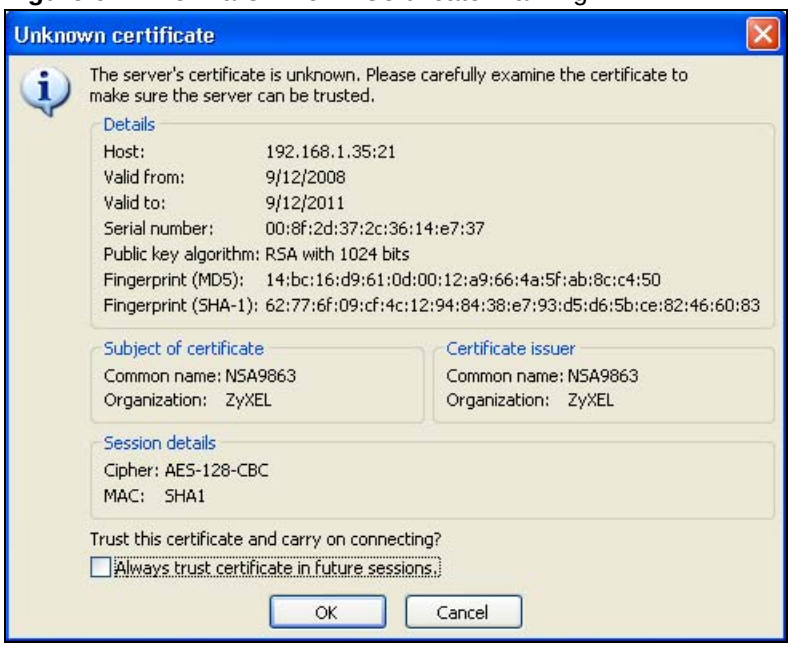
1 Open FileZilla and click **File > Site Manager > New Site**.
   - Configure the **Host** field with the NSA's address.
   - Set the **Servertype** to **FTPES - FTP over explicit TLS/SSL**.
   - Configure the account name and password.
   - Click **Connect.**

Figure 63 FileZilla Site Manager



2 A security warning screen displays. The SHA1 fingerprint must match the NSA's certificate you downloaded from the NSA to your computer. (Double-click the NSA's certificate file and then click **Details** and look at the **Thumbprint**). If they match, click **OK**.

Figure 64 FileZilla Unknown Certificate Warning



The shares and folders to which Gonzo has access display. Now you can use FTP to securely transfer files to or from the NSA. Use a secure method to let your users know the correct fingerprint for the NSA's certificate so they can check it before adding a security exception.

3.5.3 Controlling Access to Shares, Folders, and Files

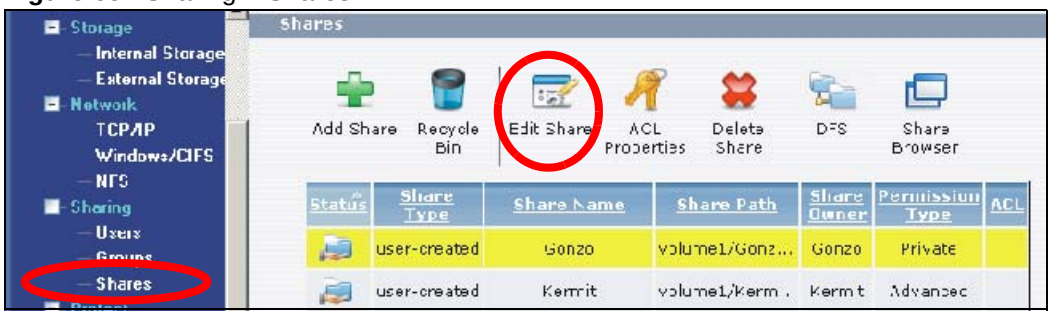
Gonzo wants to give Kermit and the senior management group read-only access to the Strategy folder. However Kermit is not to see the 2010-2014-Plans file. The following sections show how to configure the "Gonzo" share's access settings and Access Control List (ACL) settings.

3.5.3.1 Configuring the Share's Access

First you need to give Kermit and the senior management read-only access to the share.

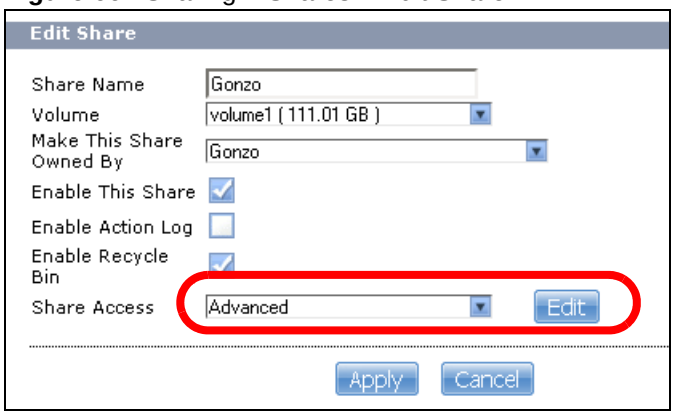
1 Click **Sharing** > **Shares**. Select the Gonzo share and click **Edit Share**.

Figure 65 Sharing > Shares



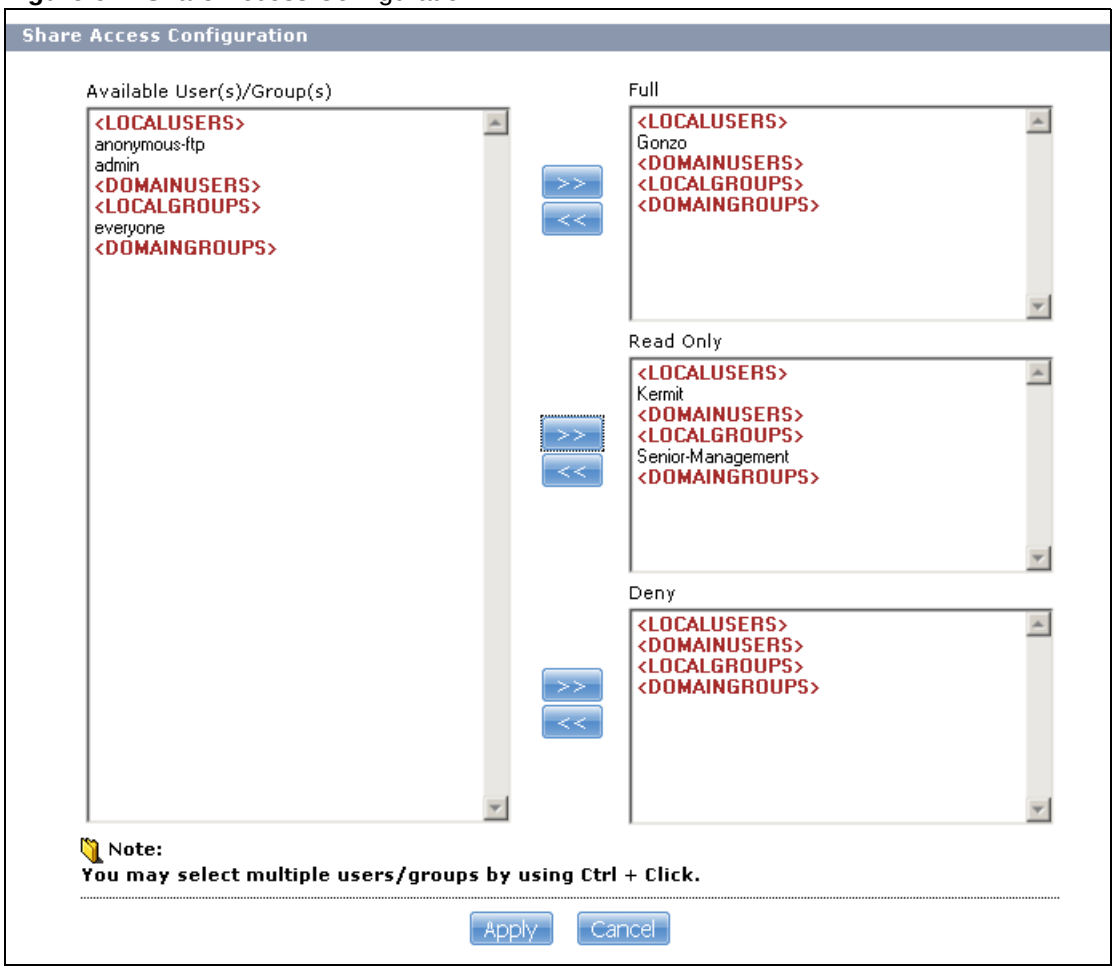
2 Set the **Share Access** to **Advanced** and click **Edit**.

Figure 66 Sharing > Shares > Edit Share



3 Move **Senior-Management** and **Kermit** to **Read Only**. Click **Apply** in this screen and again in the edit screen.

Figure 67 Share Access Configuration

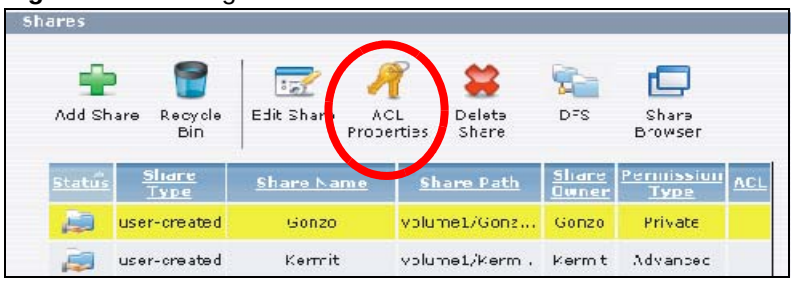


3.5.3.2 Setting the ACL to Deny Access to a File

Now you need to stop Kermit from accessing the 2010-2014-Plans file.

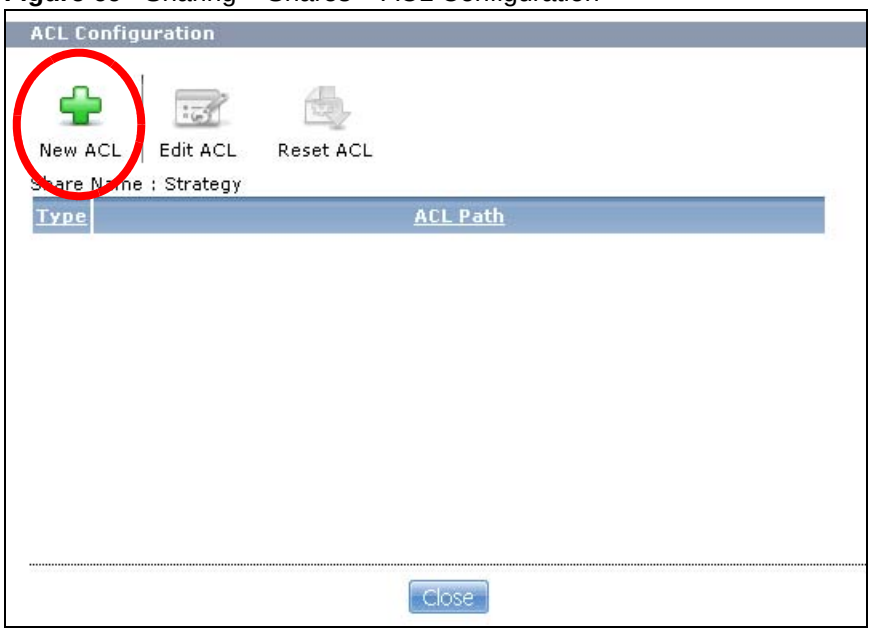
1 Select the **Gonzo** share, and click **ACL Properties**.

Figure 68 Sharing > Shares



2 Click **New ACL**.

Figure 69 Sharing > Shares > ACL Configuration

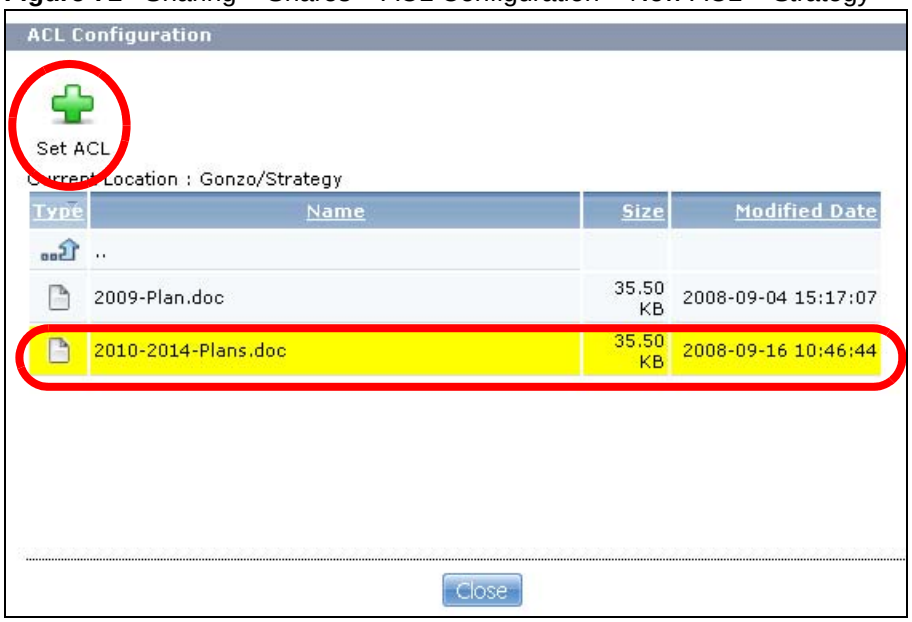


3 Open the **Strategy** folder.

Figure 70 Sharing > Shares > ACL Configuration > New ACL

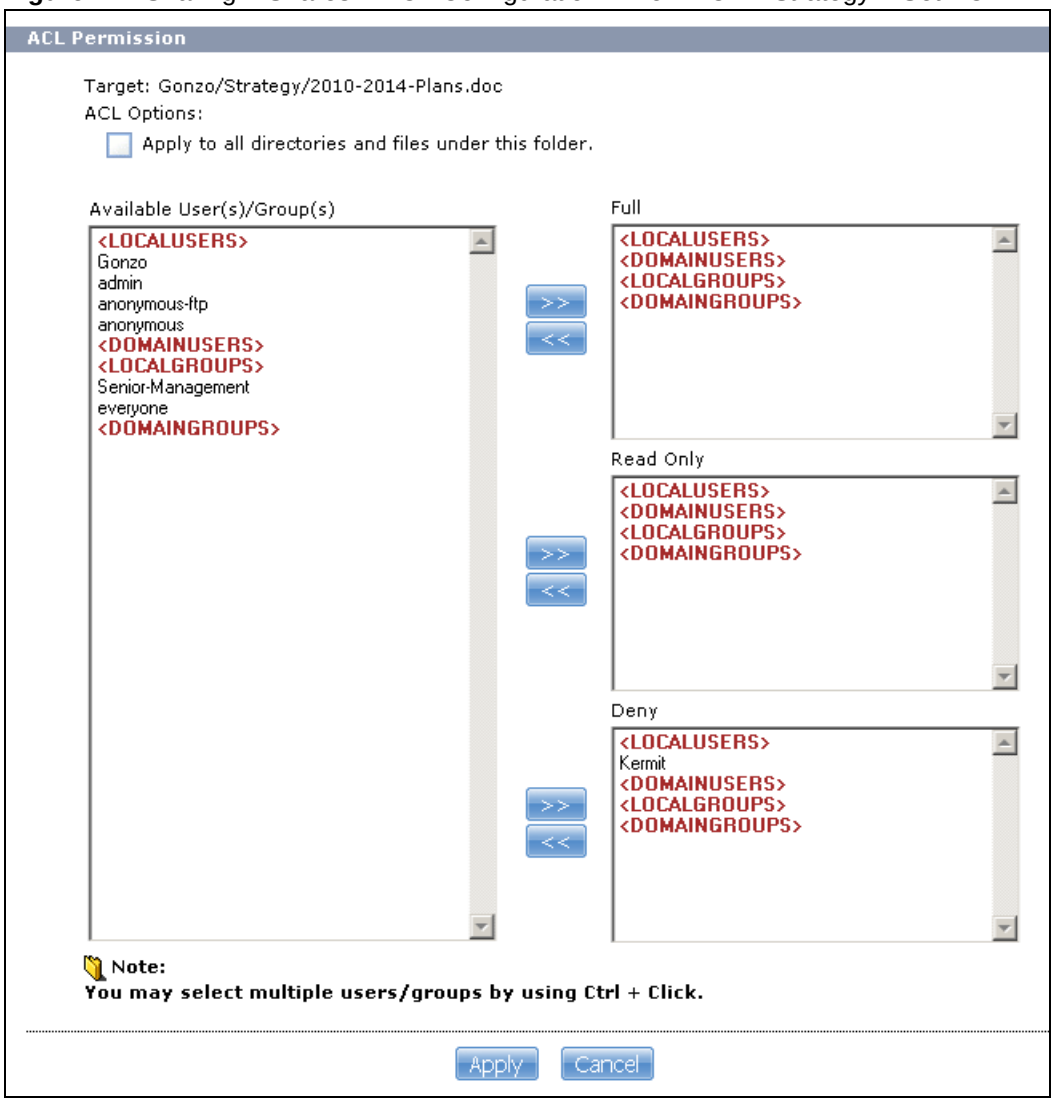
4 Select the 2010-2014-Plans.doc file and click **Set ACL**.

Figure 71 Sharing > Shares > ACL Configuration > New ACL > Strategy



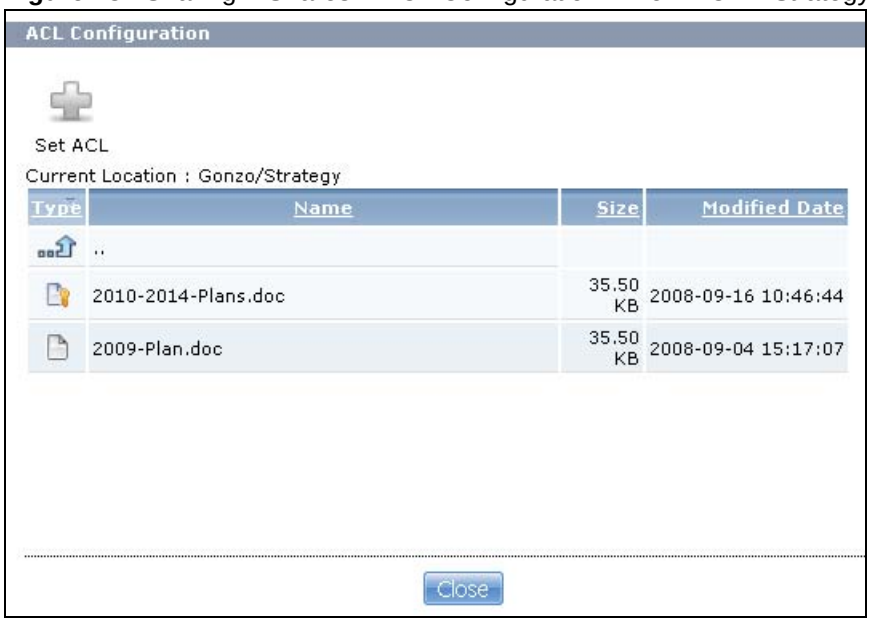
5 Move **Gonzo** to **Deny**.

Figure 72 Sharing > Shares > ACL Configuration > New ACL > Strategy > Set ACL



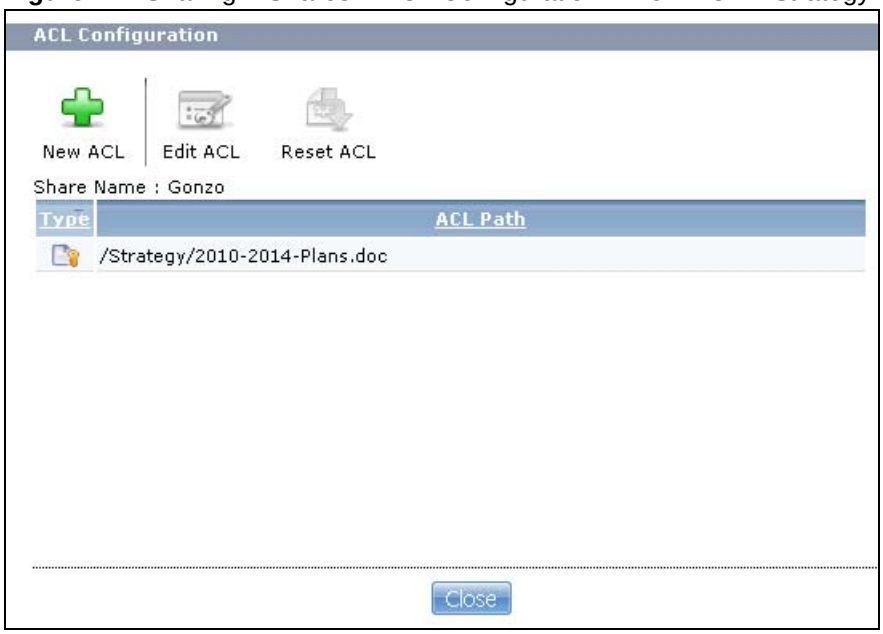
6 A **Restricted File** icon appears beside the 2010-2014-Plans.doc file. Click **Close**.

Figure 73 Sharing > Shares > ACL Configuration > New ACL > Strategy



7 This screen lists the **Strategy** share's ACLs. Click **Close**.

Figure 74 Sharing > Shares > ACL Configuration > New ACL > Strategy



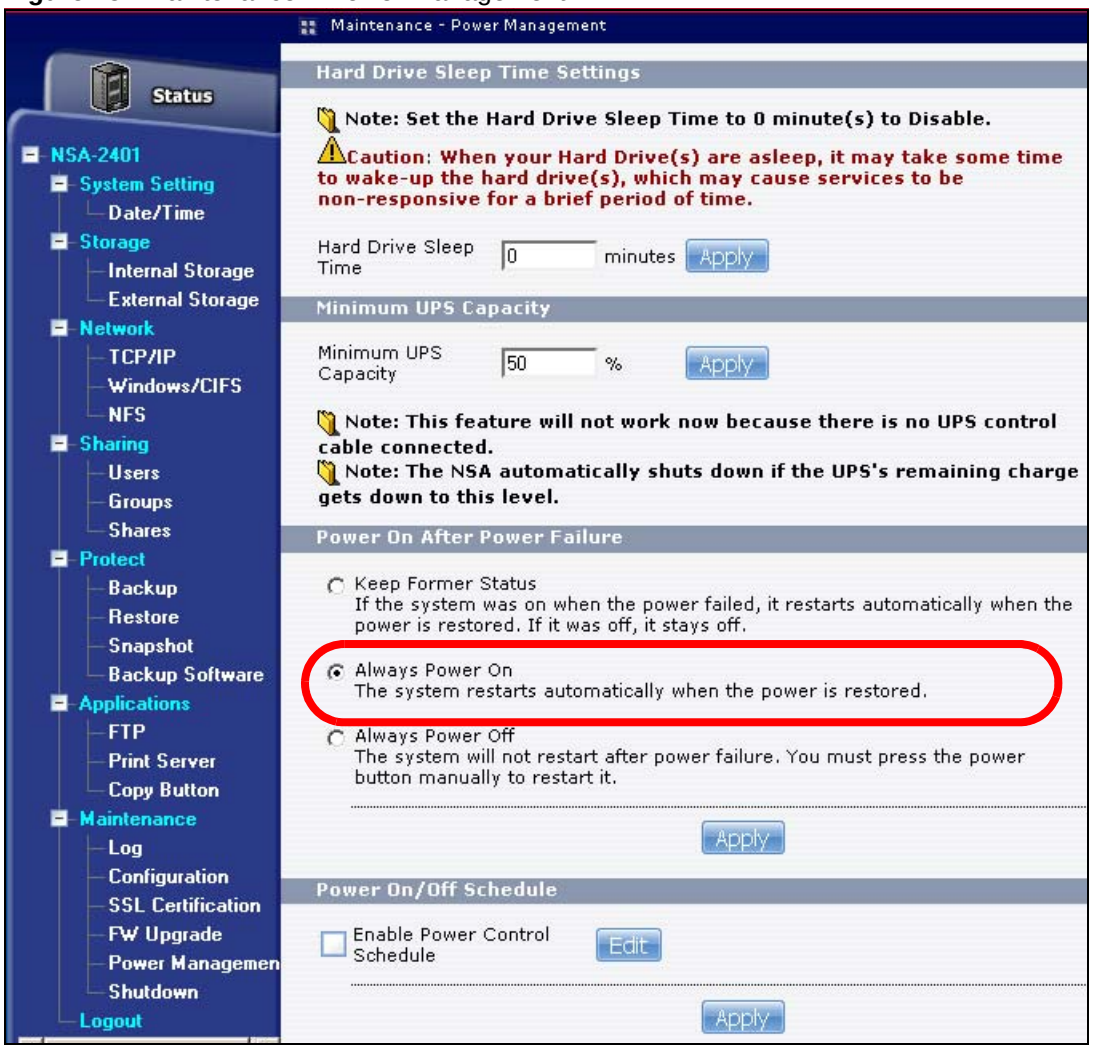
You are done configuring the 2010-2014-Plans.doc file's ACL settings. Only Gonzo can edit or delete the files in the Strategy folder. Kermit and any member of the senior management group can log into the NSA and view the contents of the Strategy folder, although Kermit cannot see the 2010-2014-Plans.doc file.

3.6 Power Resume

To keep the NSA operating as much of the time as possible, do the following to have the NSA automatically restart when the power comes back on after a power failure.

Click **Maintenance** > **Power Management**. Select **Always Power On** and click **Apply**.

Figure 75 Maintenance > Power Management



3.7 How to Use Backups and Snapshots

Use the NSA's backup and snapshot features to backup your files and folders.

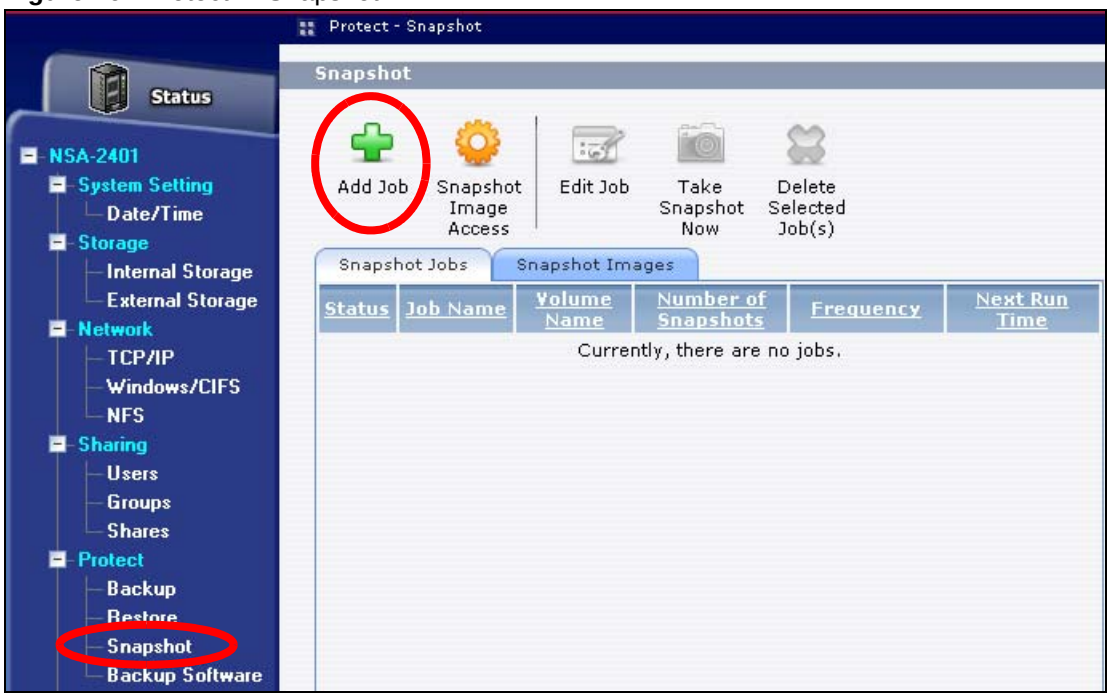
- Do snapshots frequently (hourly or daily for example) since they are faster than backups. Snapshots help protect against accidental file loss or damage caused by hackers.
- Schedule backups for times when the network is not busy (like at night or on weekends). For example, you might do daily backups of important individual files or folders and a weekly general archive. You can save backups to another location so your files can survive even if the original RAID or NSA fails.

3.7.1 Creating a Snapshot Job

Here's an example of configuring hourly snapshots for a volume.

1 Click **Protect** > **Snapshot** > **Add Job**.

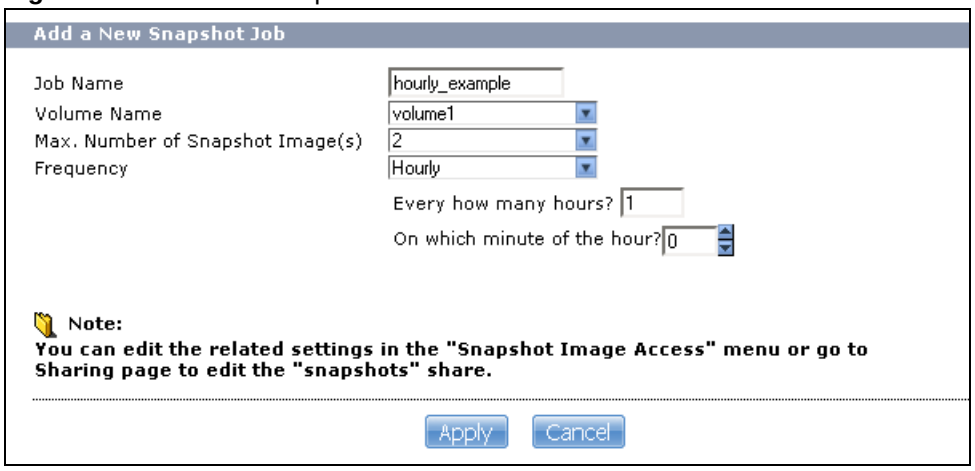
Figure 76 Protect > Snapshot



2 Enter a name for the job, select the volume of which to take snapshots, set the number of snapshot images to keep (2 in this example). For the frequency, set it to occur every hour. Click **Apply**.

It's strongly recommended to set the maximum amount of snapshots setting as low as possible as a high amount of snapshots can significantly reduce the volume's file write performance.

Figure 77 Protect > Snapshot > Add Job

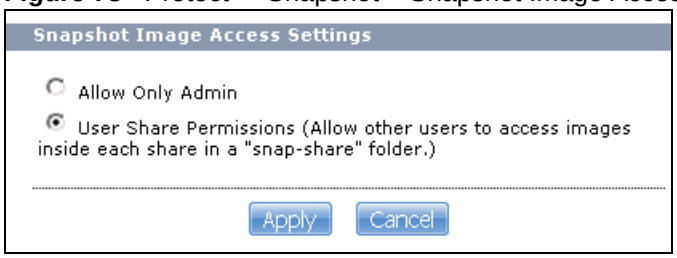


3.7.2 Configuring Snapshot Image Access

Taking a snapshot creates an image file that you use to restore files. By default, only the administrator can access the snapshot images. You want to allow users to access snapshot images in the shares that they use.

Click **Protect** > **Snapshot** > **Snapshot Image Access** to open the following screen. Then select **User Share Permissions** and click **Apply**.

Figure 78 Protect > Snapshot > Snapshot Image Access


Snapshot Image Access Settings
Allow Only Admin
User Share Permissions (Allow other users to access images inside each share in a "snap-share" folder.)
Apply
Cancel

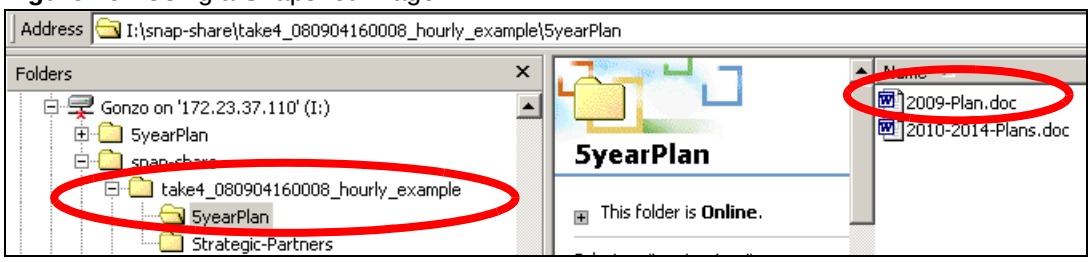
3.7.3 Using a Snapshot Image to Restore Files

To use a snapshot to restore files, use the MyNSA screens, CIFS (Windows Explorer), or FTP to browse to the folder named "snap-share". Open or copy the folder or file that you want to restore.

For example, Gonzo accidently overwrote his 2009-Plan.doc file.

Use Windows Explorer to browse to the Gonzo share. (The Quick Start Guide covers how to map a share to a Windows network drive).

Figure 79 Using a Snapshot Image



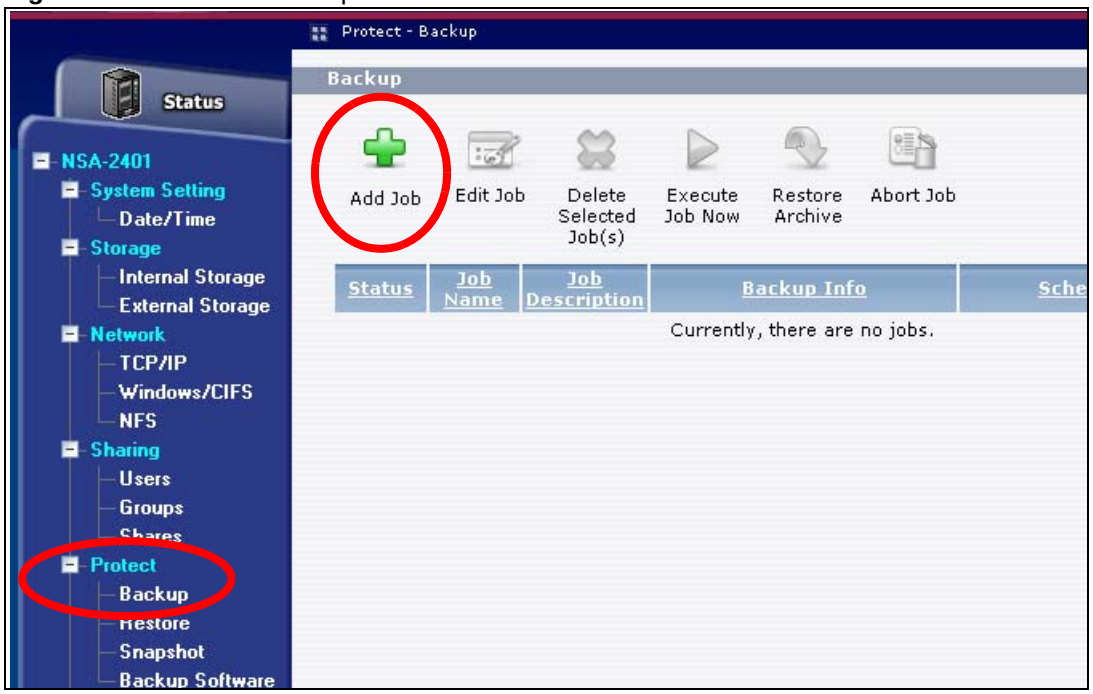
- There is a snap-share folder with a folder for each snap-shot of volume contents to which Gonzo has access. A snap-shot folder's name identifies the take number of the individual snapshot, the time the snapshot was taken (in year month, day, hour, minute, second format) and the name of the snapshot job.
- The take4_080904160008_hourly_example folder contains a 5yearPlan folder with a 2009-Plan.doc file. Gonzo can open the 2009-Plan.doc file or copy it to another location.

3.7.4 Creating a Synchronization Backup

Gonzo has an important folder that the German branch office uses on a daily basis. Because Gonzo updates the files frequently, you decide to create a backup job that has the NSA publish the contents of the folder to an NSA in the German branch office. To create a synchronization backup:

1 Click **Protect** > **Backup** > **Add Job**.

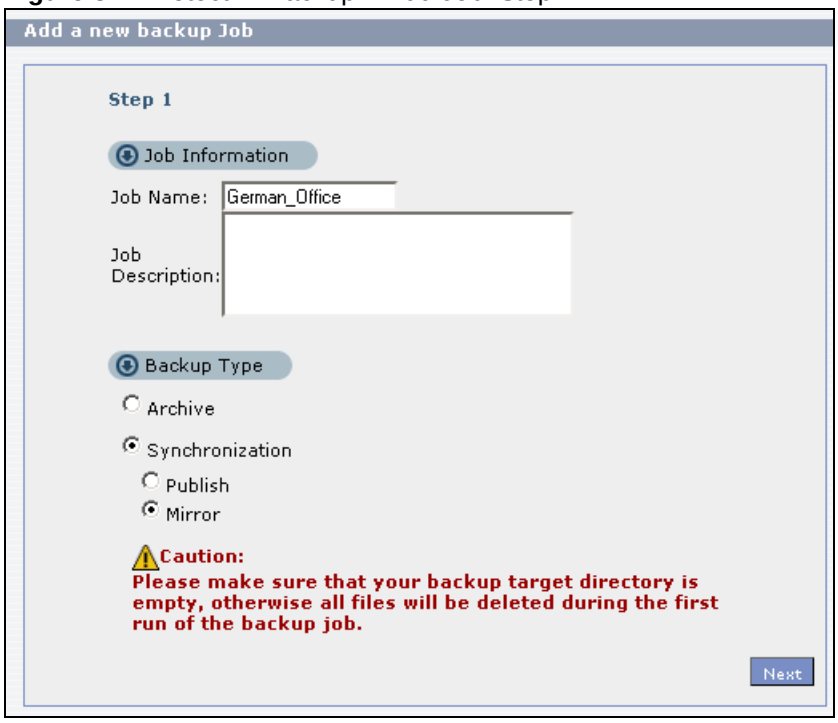
Figure 80 Protect > Backup



2 Name the backup job and select **Synchronization**.

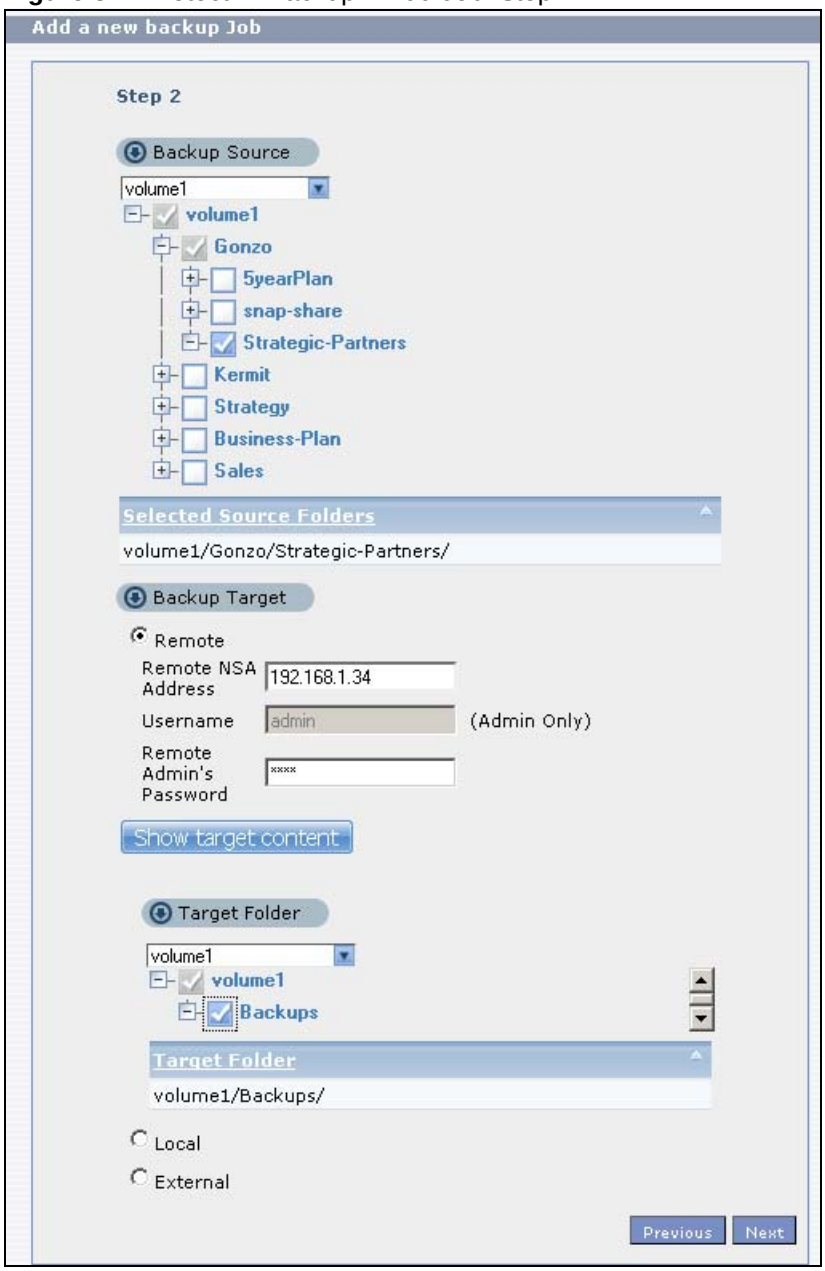
Gonzo wants only his current set of files in the remote NSA's folder, so you select **Mirror** to make the target folder identical to the source folder. The NSA deletes any other files in the target folder.

Figure 81 Protect > Backup > Add Job: Step 1



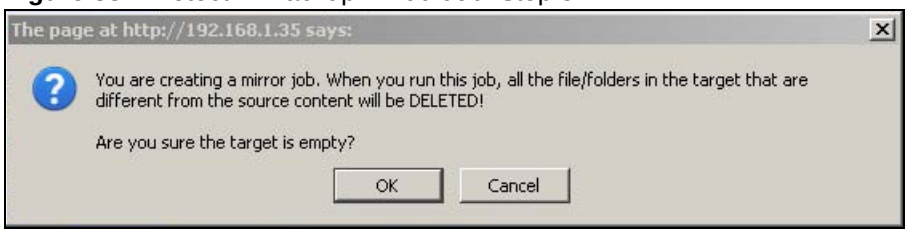
3 Select the folder that needs to be mirrored (the Gonzo share's **Strategic-Partners** folder in this example) and **Remote**.
   - Enter the other NSA's address and administrator password.
   - Click **Show target content** to display the remote NSA's contents.
   - Select the destination on the remote NSA (**Backups** in this example).
   - Click **Next**.

Figure 82 Protect > Backup > Add Job: Step 2



4 Click **OK** in the warning dialog box.

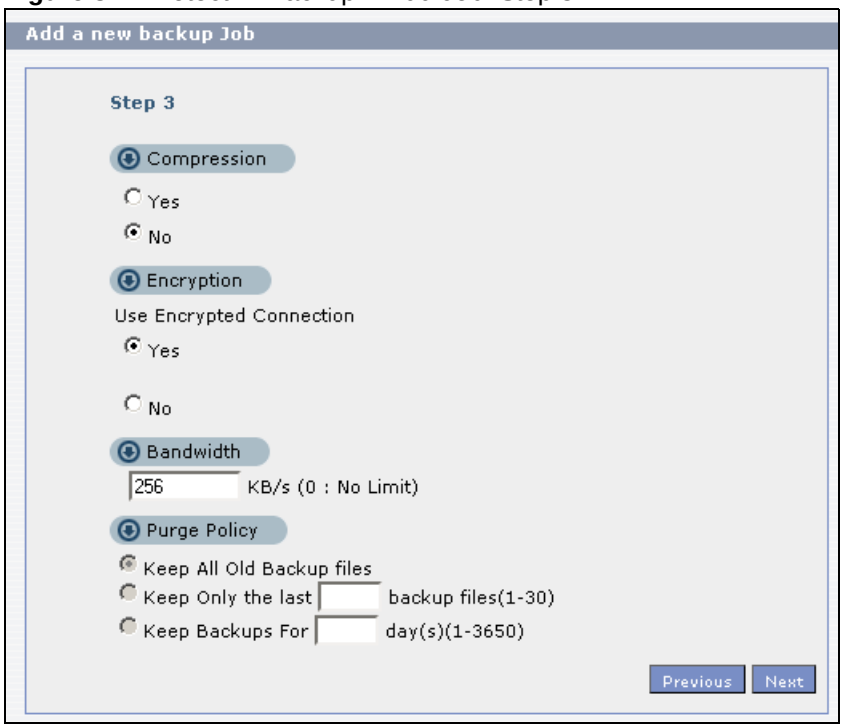
Figure 83 Protect > Backup > Add Job: Step 3


The page at http://192.168.1.35 says:
You are creating a mirror job. When you run this job, all the file/folders in the target that are different from the source content will be DELETED!
Are you sure the target is empty?
OK
Cancel

5 For this example, assume the connection to the German branch office is a good one and not many files need to be backed up so leave the compression off.

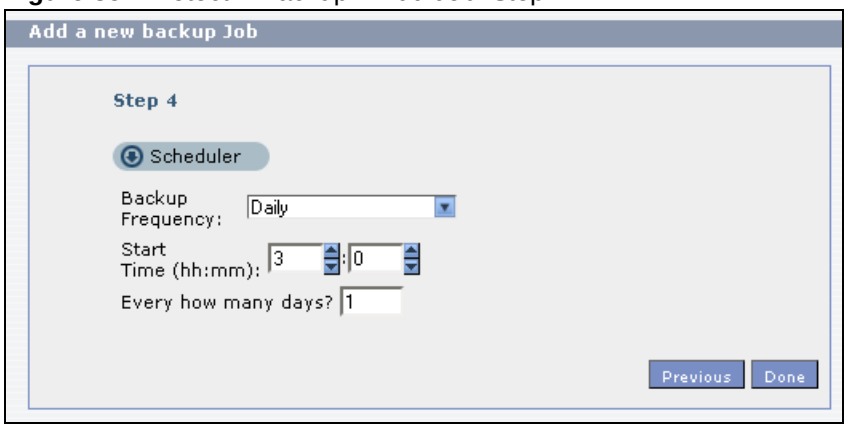
- Turn on the encryption to protect these sensitive files during the transfer. The final files stored on the remote NSA will be unencrypted (usable).
- Restrict the bandwidth usage to 256 KB/s to stop the archives from using all of your network connection's available bandwidth.
- You don't have to configure a purge policy for a synchronization backup.
- Click **Next**.

Figure 84 Protect > Backup > Add Job: Step 3



6 Schedule the backup to occur every morning at 3:00 and click **Done**.

Figure 85 Protect > Backup > Add Job: Step 4



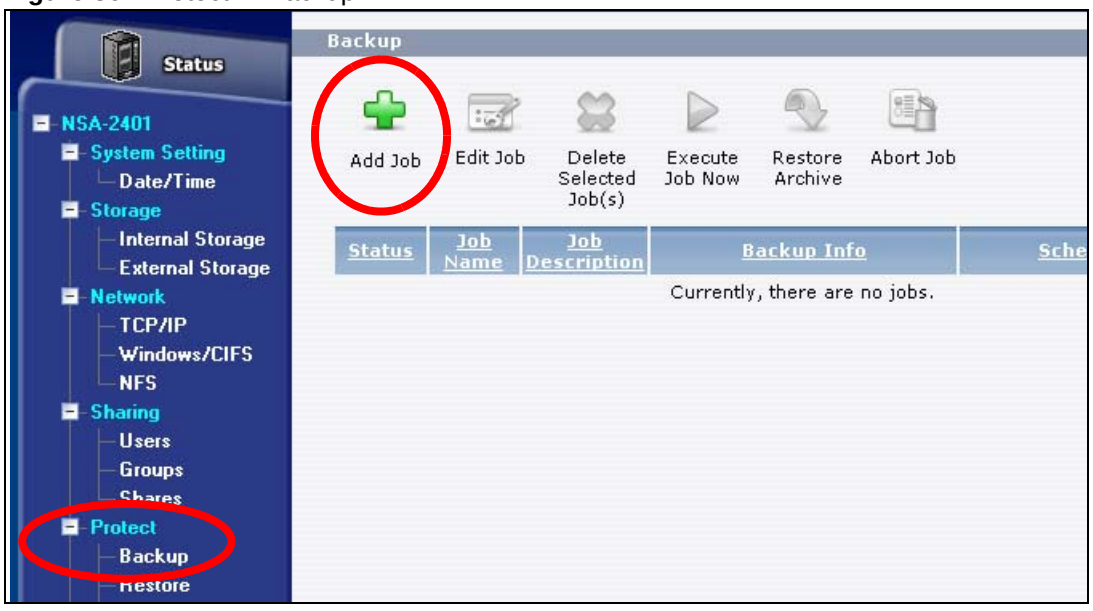
You do not need to use a special restore process to use the files a synchronization backup creates. The copy of files that the NSA creates on the other NSA's Backups share can be used directly by anyone with access to that share.

3.7.5 Creating an Archive Backup

To backup the NSA every week to a remote NSA:

1 Click **Protect** > **Backup** > **Add Job**.

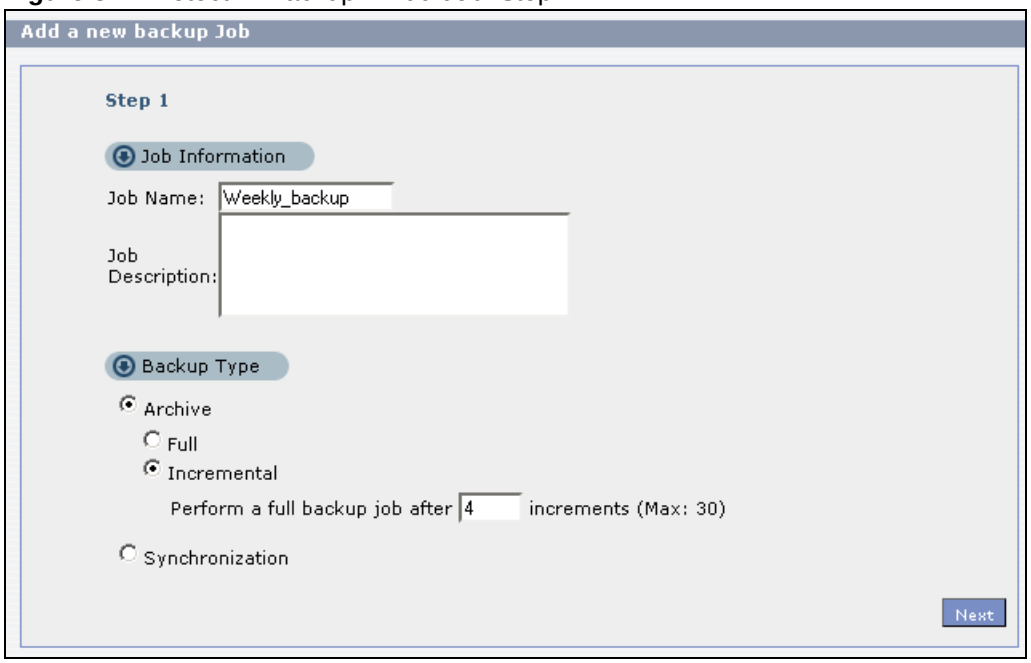
Figure 86 Protect > Backup



2 Identify the backup job and select **Archive**.

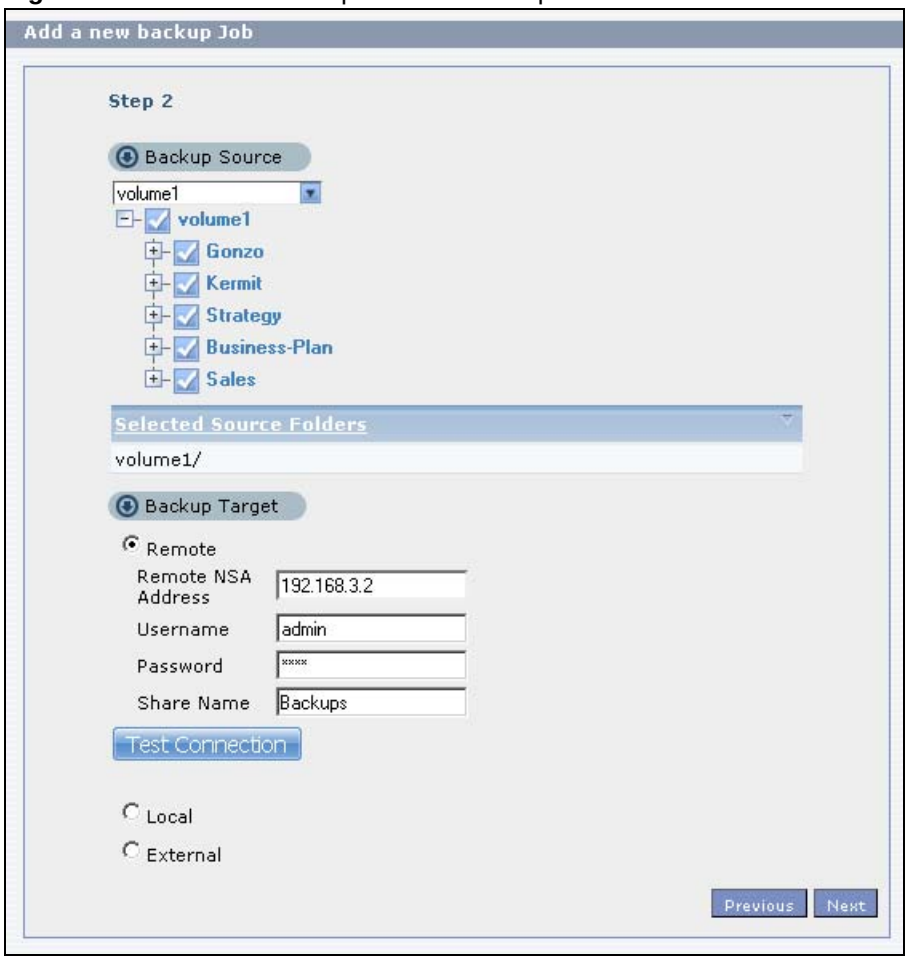
New files are often added to the shares that you need to back up and existing files are not frequently changed so select **Incremental**. The NSA does a full backup first and later only copies source files that are new and/or modified since the last backup. This example sets the NSA to do another full backup after every four incremental backups.

Figure 87 Protect > Backup > Add Job: Step 1



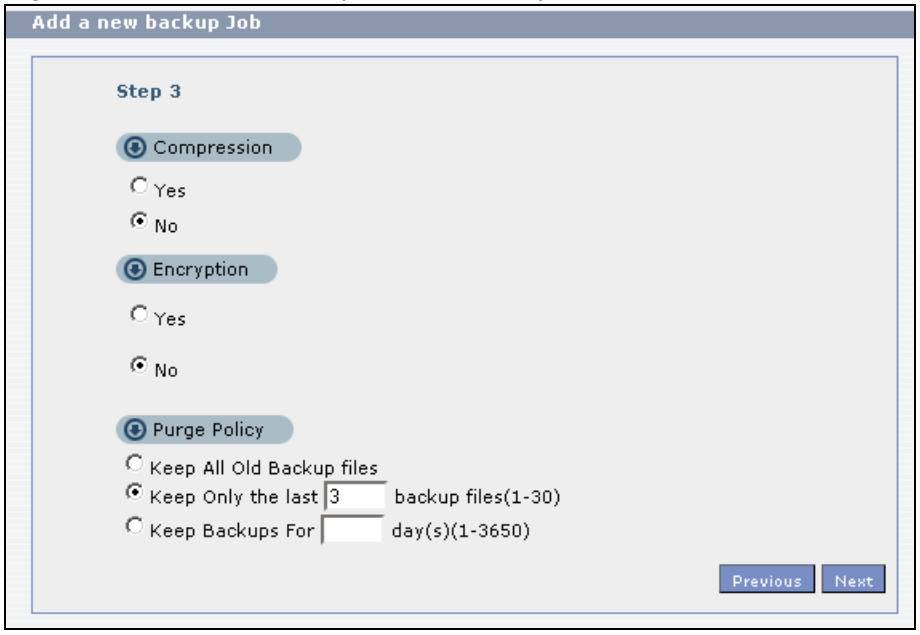
3 Select the **volume1** check box to select all the folders and files.
Select **Remote** and enter the other NSA's address, username, password, and share name.
If you want to make sure the remote NSA is reachable, click **Test Connection**.

Figure 88 Protect > Backup > Add Job: Step 2



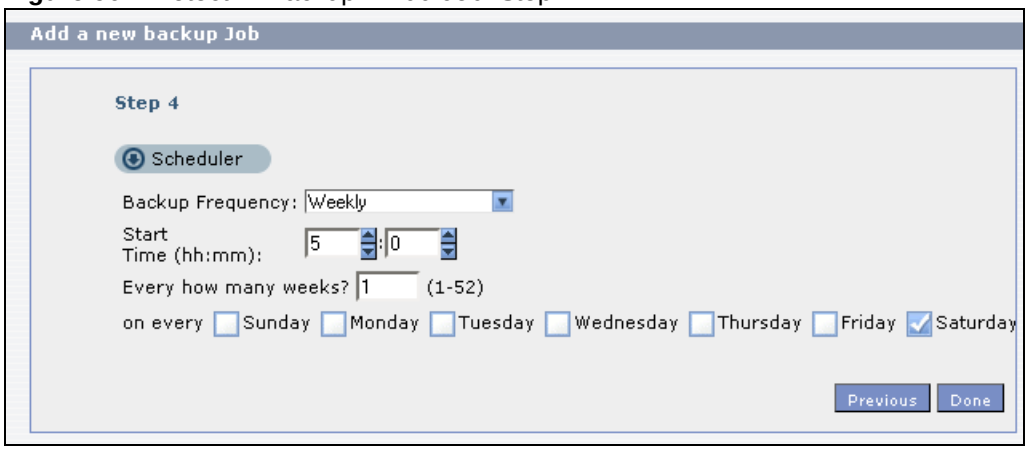
4 In this example, the target NSA is on the LAN so leave the compression off.
Security is already configured on the target NSA so you can leave the encryption off, too.
Have the NSA keep 3 backups.

Figure 89 Protect > Backup > Add Job: Step 3



5 Set the frequency to **Weekly**. Schedule the backup for 5:00 every Saturday morning.

Figure 90 Protect > Backup > Add Job: Step 4

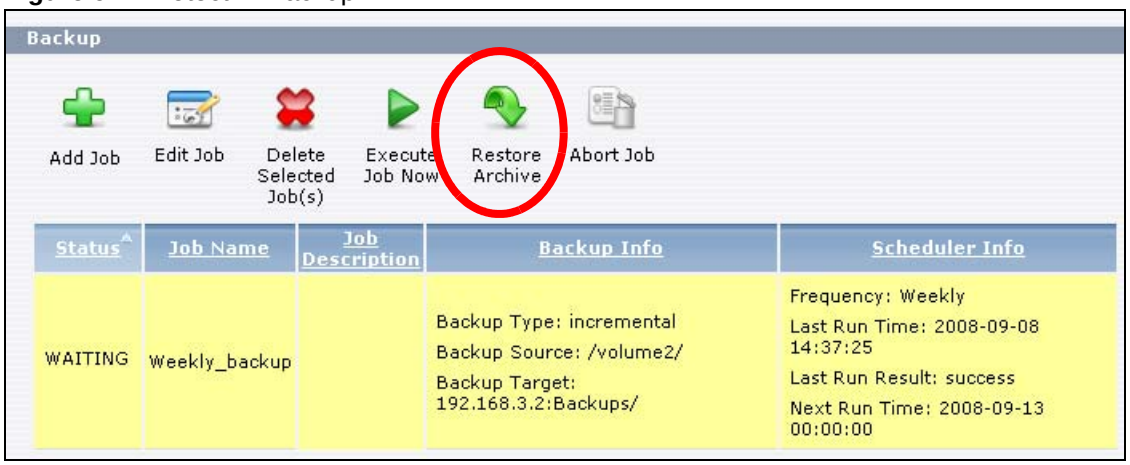


3.7.6 Restoring Archived Files by Backup Job

If you have backup jobs for which the NSA has already performed backups, you can restore the files based on the backup job. Gonzo accidently deleted all of the files in his share and needs to do the following to restore them.

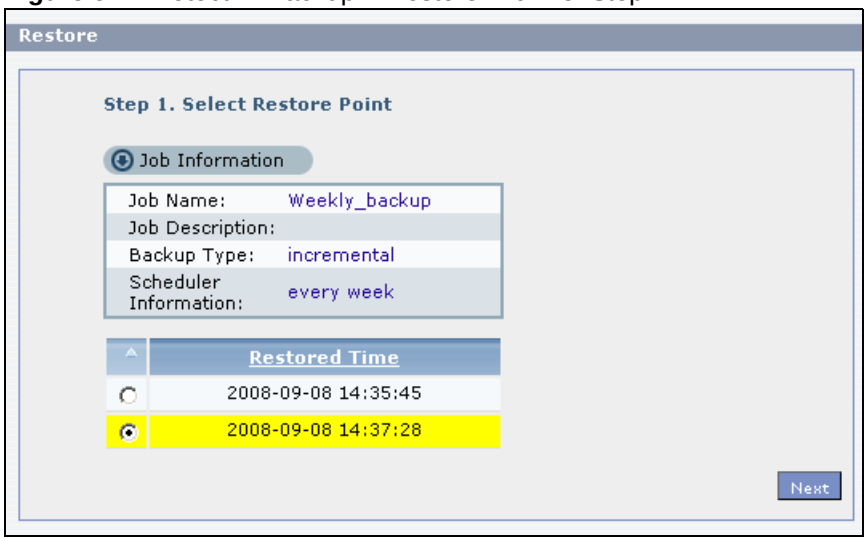
1 Click **Protect** > **Backup** screen, select a backup job and click **Restore Archive**.

Figure 91 Protect > Backup



2 Select which backup to use and click **Next**.

Figure 92 Protect > Backup > Restore Archive: Step 1

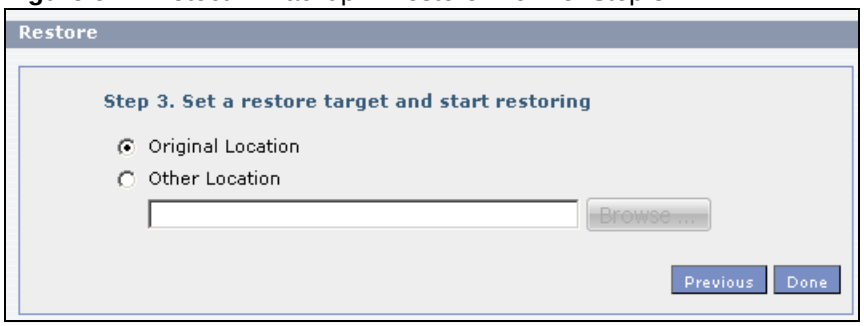


3 Select the Gonzo share and click **Next**.

Figure 93 Protect > Backup > Restore Archive: Step 2

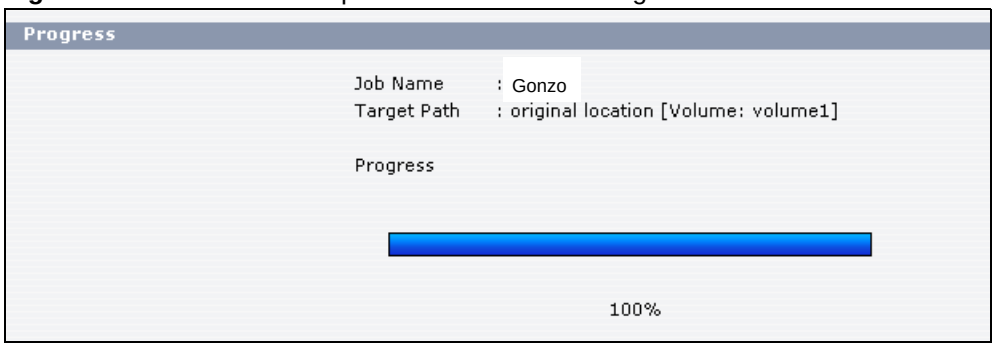
4 Select the original location and click **Done**.

Figure 94 Protect > Backup > Restore Archive: Step 3



5 The NSA restores the files into the Gonzo share. When it finishes you can access the files.

Figure 95 Protect > Backup > Restore Archive: Progress

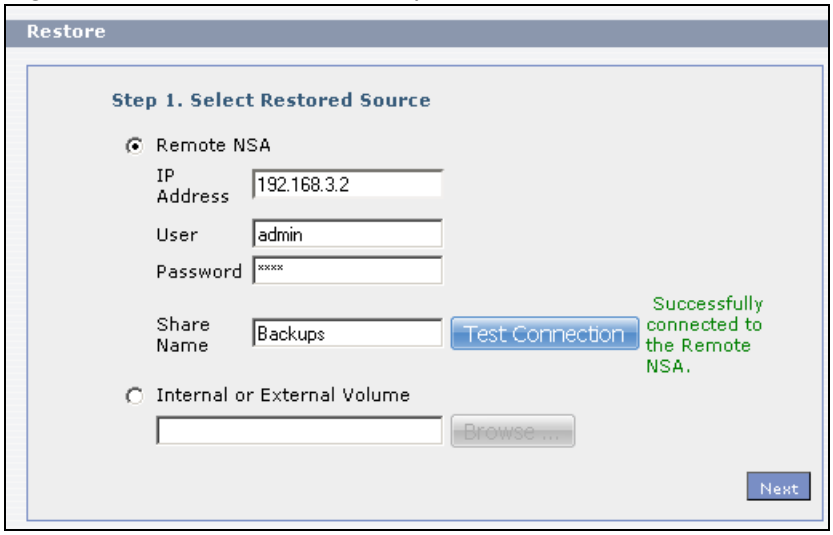


3.7.7 Restoring by Backup Files

If you deleted an archive backup job or the NSA or the RAID array containing the backup job failed you cannot restore archived files by the backup job. In this example, the NSA's RAID array failed. You've replaced the hard drives and re-configured the RAID. To restore by backup files:

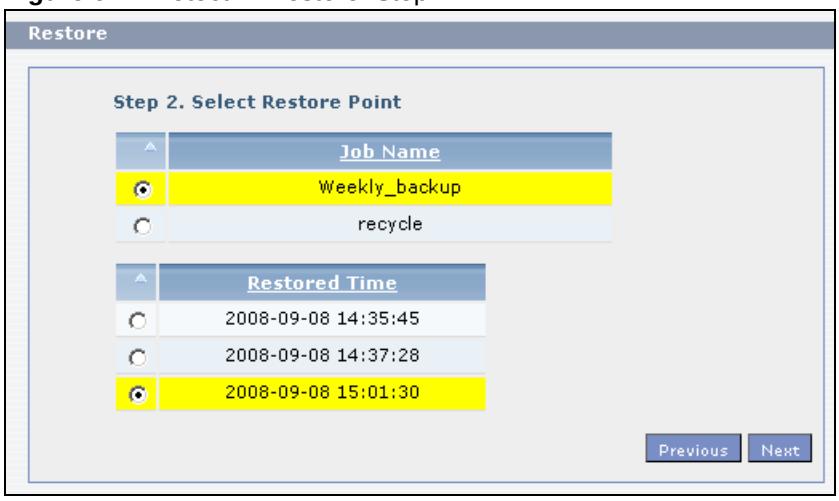
1 Click **Protect** > **Restore**. Specify where the archive files are located. In this example, enter "192.168.3.2" as the IP address, "admin" as the account name, "1234" as the password, and "Backups" as the share name. Click **Test Connection**. Click **Next.**

Figure 96 Protect > Restore: Step 1



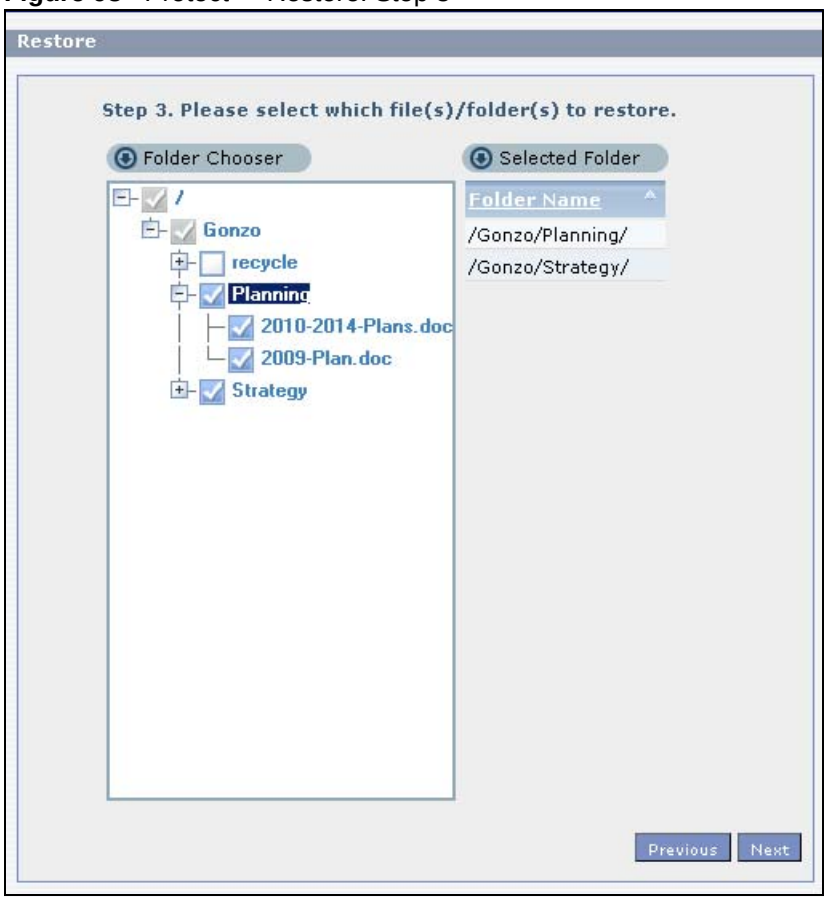
2 Select the backup job and backup time and click **Next**.

Figure 97 Protect > Restore: Step 2



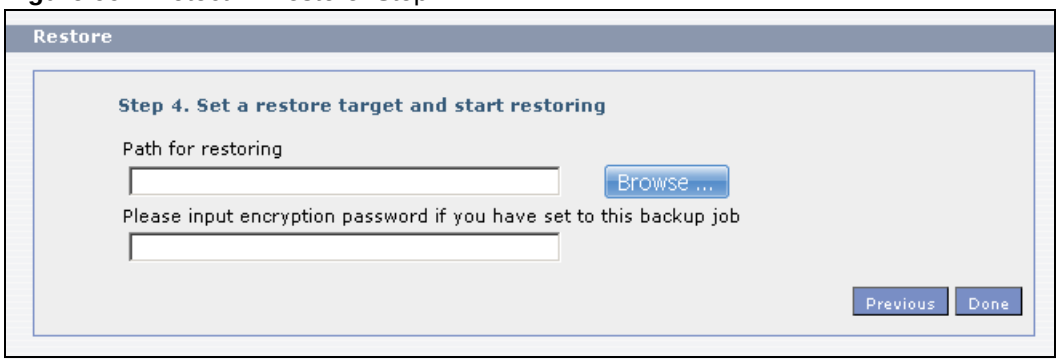
3 Select everything in the Gonzo share except the recycle folder. Click **Next**.

Figure 98 Protect > Restore: Step 3



4 Specify where you want to put the files. Browse to "/Gonzo". Click **Done**.

Figure 99 Protect > Restore: Step 4


Restore
Step 4. Set a restore target and start restoring
Path for restoring
Browse ...
Please input encryption password if you have set to this backup job
Previous
Done

The NSA restores the files and you can use them again.

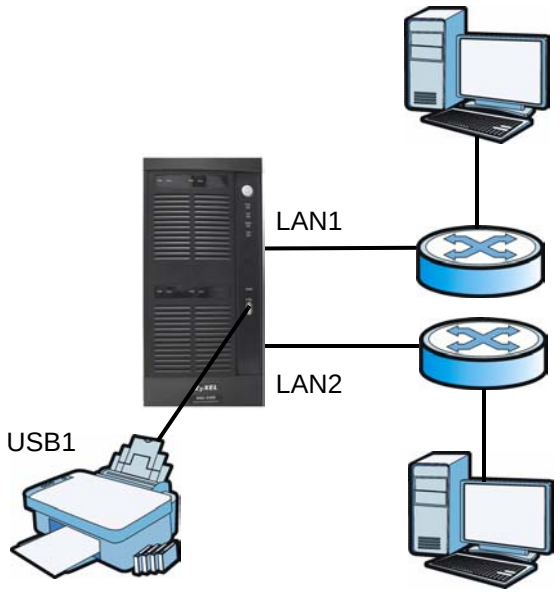
3.8 Printer Server Tutorial

Do the following to configure the NSA to allow computers on your network to share a printer. See www.zyxel.com for a list of compatible printers.

1 Make sure the NSA is on and the **SYS** light shines steadily.

2 Use a USB cable to connect the printer's USB port to one of the NSA's USB ports. Make sure the printer is also connected to an appropriate power source.

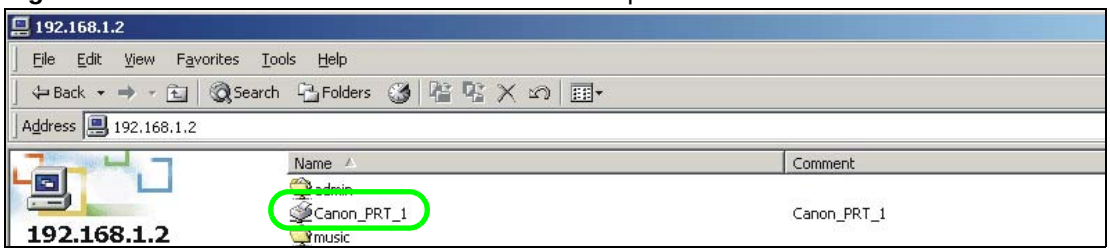
Figure 100 Printer Sharing



3 Turn on the printer. The NSA detects it after a few moments.

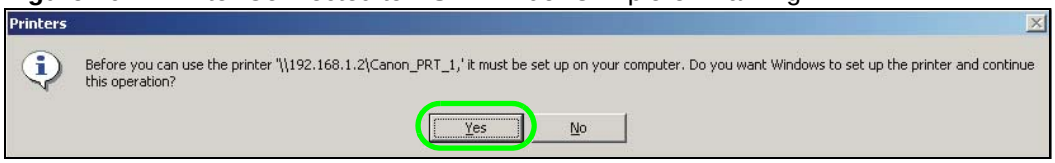
4 On your computer, open your CIFS file sharing program (Windows Explorer for example) and browse to the NSA. Double-click the printer's icon.

Figure 101 Printer Connected to NSA: Windows Explorer



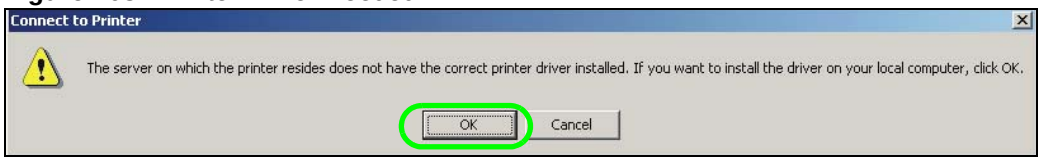
5 If you get a warning screen, click the option that lets you continue (**Yes** in this example).

Figure 102 Printer Connected to NSA: Windows Explorer Warning


Printers
Before you can use the printer '\\192.168.1.2\Canon_PRT_1,' it must be set up on your computer. Do you want Windows to set up the printer and continue this operation?
Yes
No

6 If your computer does not already have the printer's driver installed, you will need to install it. In this example, click **OK**.

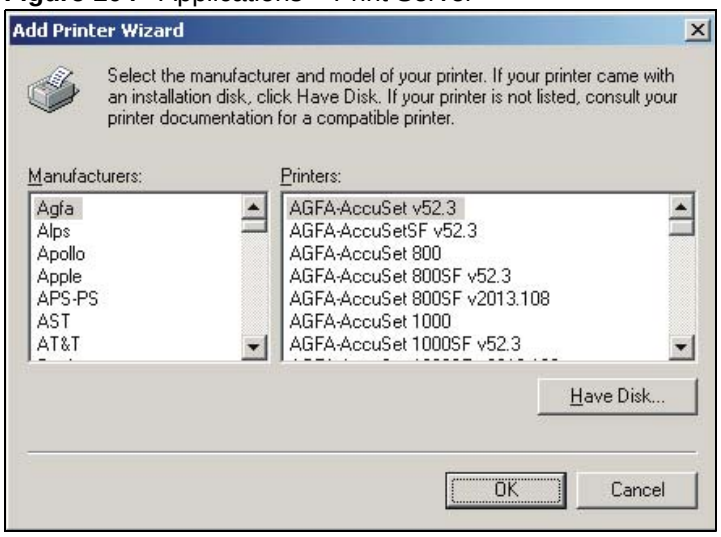
Figure 103 Printer Driver Needed


Connect to Printer
The server on which the printer resides does not have the correct printer driver installed. If you want to install the driver on your local computer, click OK.
OK
Cancel

7 Use the wizard screens to install the printer driver on the computer. You may need to get the file from the printer's CD or the printer manufacturer's website (the driver is not installed on the NSA).

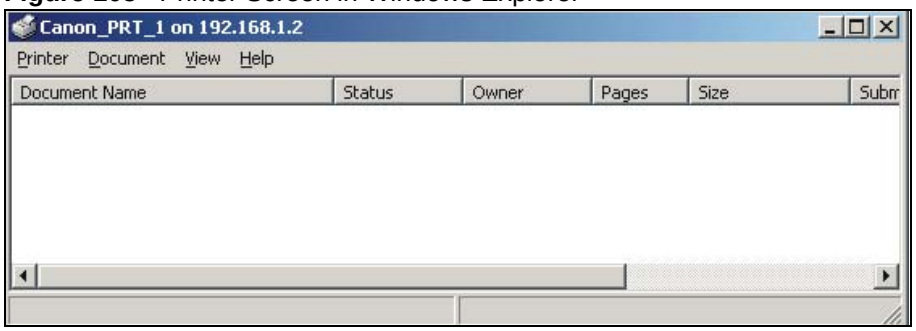
You must install the printer driver on each computer that will use the printer.

Figure 104 Applications > Print Server



After the driver installation finishes, the computer is ready to use the printer. Select the printer in an application to use it to print. Browse to the NSA using a CIFS program (like Windows Explorer) and double-click the printer's icon to open the printer's queue of print jobs.

Figure 105 Printer Screen in Windows Explorer



Repeat steps 4 to 7 on your other computers so they can also use the printer.

3.9 How to Increase the NSA's Storage Capacity

As time goes by your company is likely to need more storage capacity. You can do one or more of the following to increase the NSA's storage capacity:

- Connect external USB hard drives
- Add internal hard drives if there are not four already installed.
- Migrate a RAID 5 array to higher capacity hard drives.

3.9.1 Connecting External USB Hard Drives

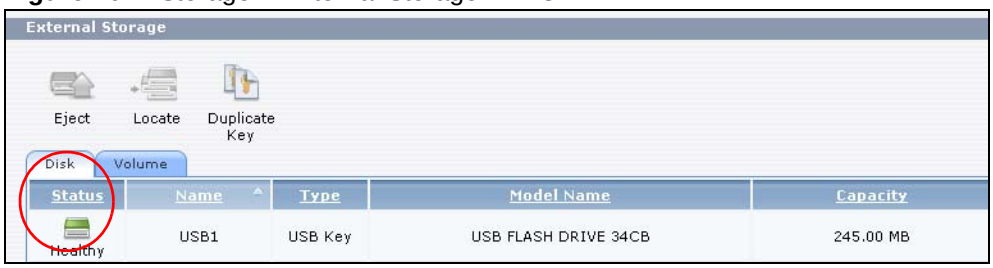
The easiest way to increase the NSA's storage capacity is to connect an external USB hard drive. External USB hard drives are great for providing storage capacity for scheduled backups and snapshots of internal volumes. (External volumes can be the destination for a scheduled backup or snapshot, but only an internal volume can be the source.) Use the following procedure.

1 Connect the external USB hard drive to **USB1** or **USB2** on the NSA's front panel.

Figure 106 Connecting a USB Hard Drive

2 Click **Storage** > **External Volumes** and make sure the USB drive displays with a healthy status.

Figure 107 Storage > External Storage > Disk



The NSA automatically creates volumes for the USB drive. You just need to configure sharing settings (Chapter 8 on page 173) to let your users use it.

3.9.2 Adding an Internal Hard Drive to an Existing Disk Array

If you do not already have four disks installed, you can install more. You can add a new disk to an existing JBOD array or three-disk RAID 5 array. When you add a new disk to an existing array, you do not have to create new volumes and sharing settings.

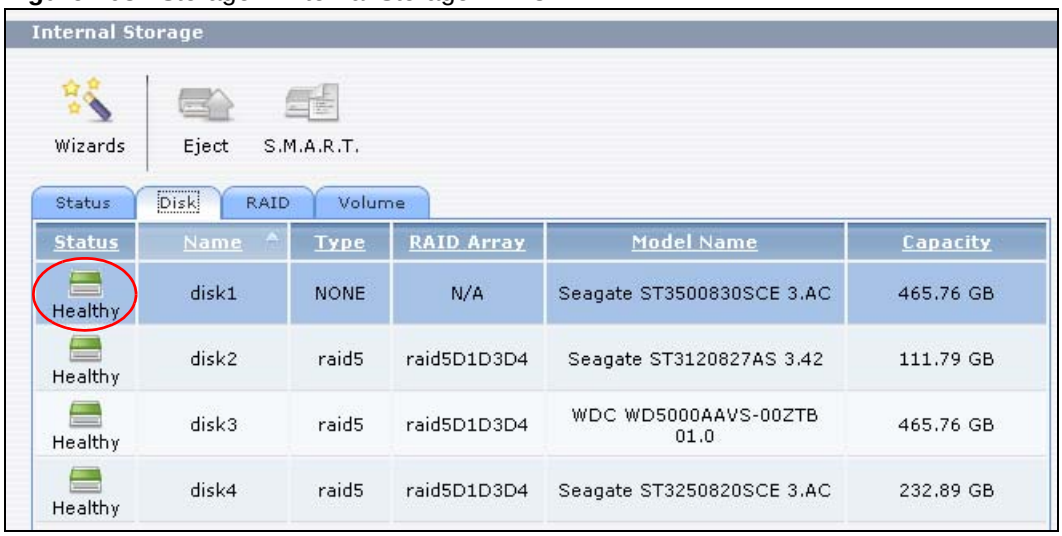
For optimal performance and RAID storage capacity, use hard drives of the same speed and capacity.

If the new hard drives have any data you want to keep, back it up to another location before you install them. Adding these hard drives to a disk array formats them so all data stored on them will be lost.

1 See the Quick Start Guide for details on installing hard drives in the NSA's bays. You can install hard drives while the NSA is operating.

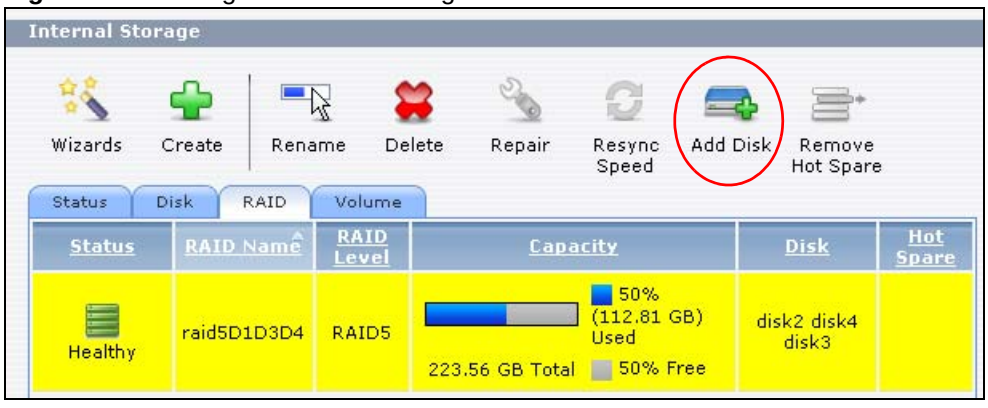
2 Click **Storage** > **Internal Volumes** > **Disk** and make sure the new drive displays with a healthy status.

Figure 108 Storage > Internal Storage > Disk



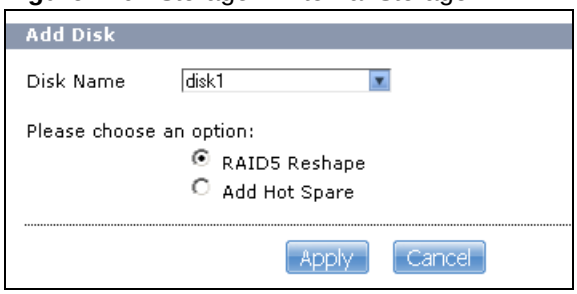
3 Click the **RAID** tab to display the RAID array summary screen. Select the array to which you want to add the disk and click **Add Disk**.

Figure 109 Storage > Internal Storage > RAID



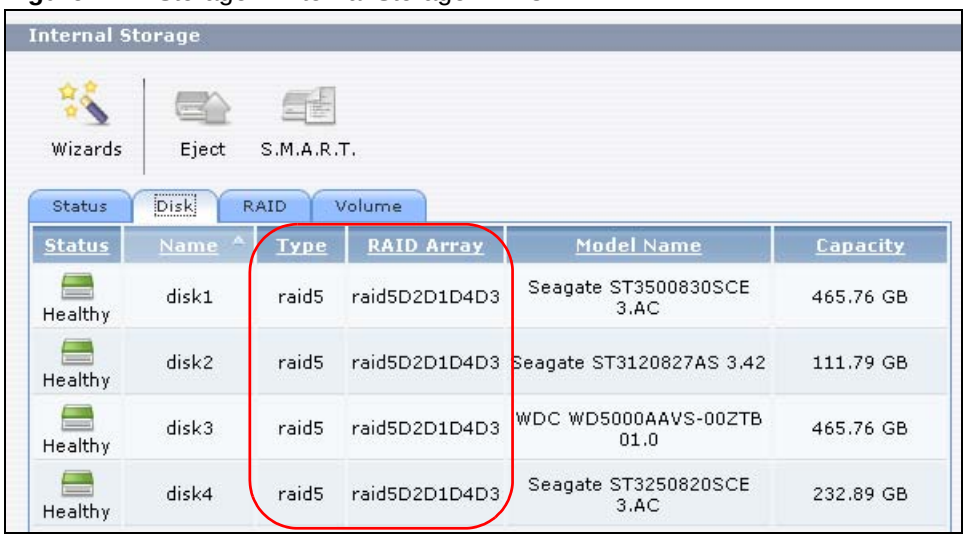
4 Select **RAID5 Reshape** and click **Apply**.

Figure 110 Storage > Internal Storage > RAID > Add Disk



5 After the NSA finishes adding the disk to the array, click the **Disk** tab. The new disk displays the same **Type** and **RAID Array** as the other disks in the array.

Figure 111 Storage > Internal Storage > Disk



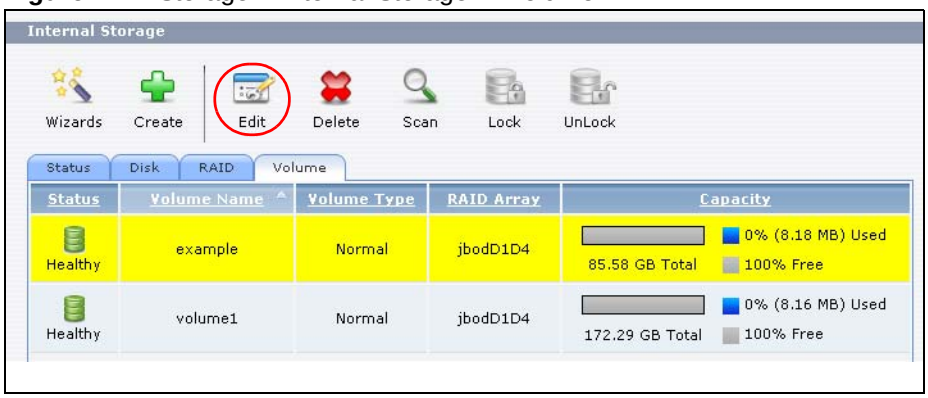
You have completed adding the hard drive to the RAID array. Continue to Section 3.9.3 on page 109 for how to use the increased storage capacity.

3.9.3 Using a Disk Array's Increased Capacity

After you increase an array's storage capacity, use the following procedure to make the NSA's existing volumes larger in order to use the increased capacity. You do not have to change your existing share, backup, and snapshot settings. Of course you can also create new volumes, but you must configure new share settings in order to use them and new backup and snapshot settings to protect the files.

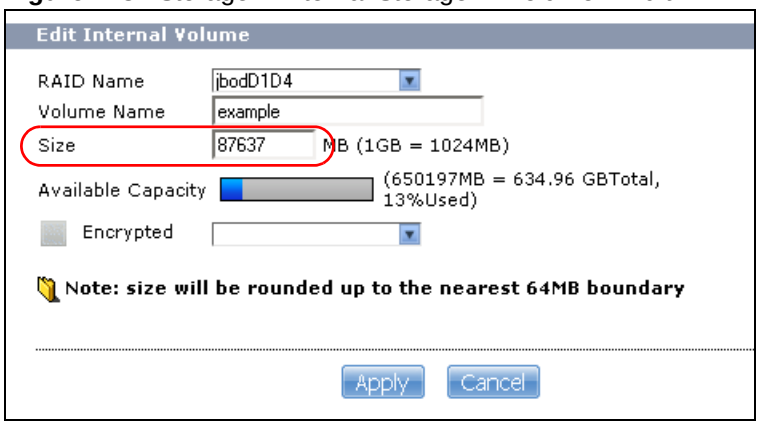
1 Click the **Volume** tab. Select a volume and click **Edit**.

Figure 112 Storage > Internal Storage > Volume



2 Increase the size and click **Apply**.

Figure 113 Storage > Internal Storage > Volume > Edit



3 Repeat these steps for other volumes that need more storage capacity.

3.9.4 Migrating a RAID to Higher Capacity Hard Drives

You can migrate a RAID 5 array to hard drives of higher capacity. Replace one hard drive at a time and recover the RAID before you go on to replace another hard drive.

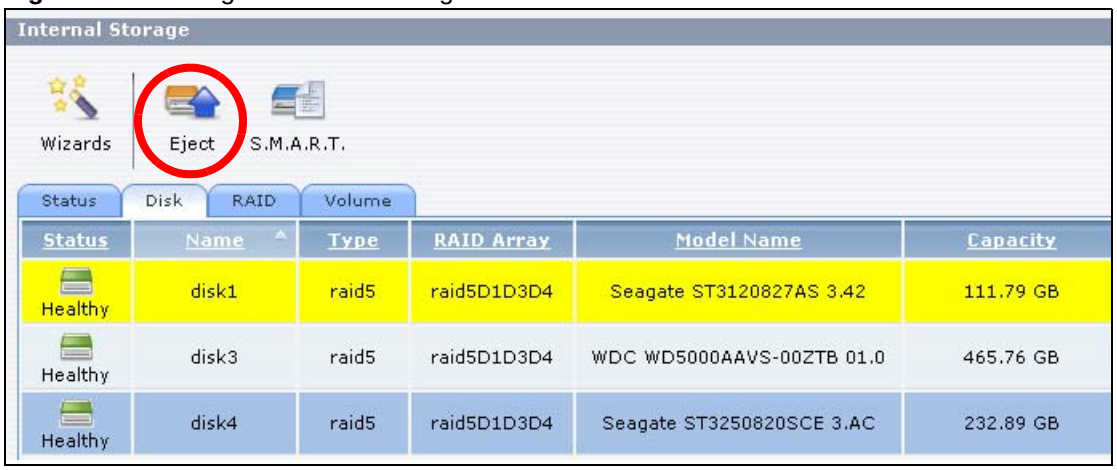
For optimal performance and RAID storage capacity, use hard drives of the same speed and capacity. It is also recommended that you perform the upgrade when the network's traffic levels are low.

If the new hard drives have any data you want to keep, back it up to another location before you install them. Adding these hard drives to a disk array formats them so all data stored on them will be lost.

To migrate a RAID5 array to a higher capacity hard drive:

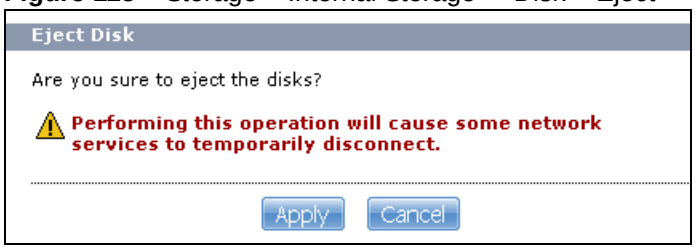
1 Click **Storage** > **Internal Storage** > **Disk** to list the installed disks. Select a disk to replace first (disk 1 in this example) and click **Eject**.

Figure 114 Storage > Internal Storage > Disk



2 Click **Apply**.

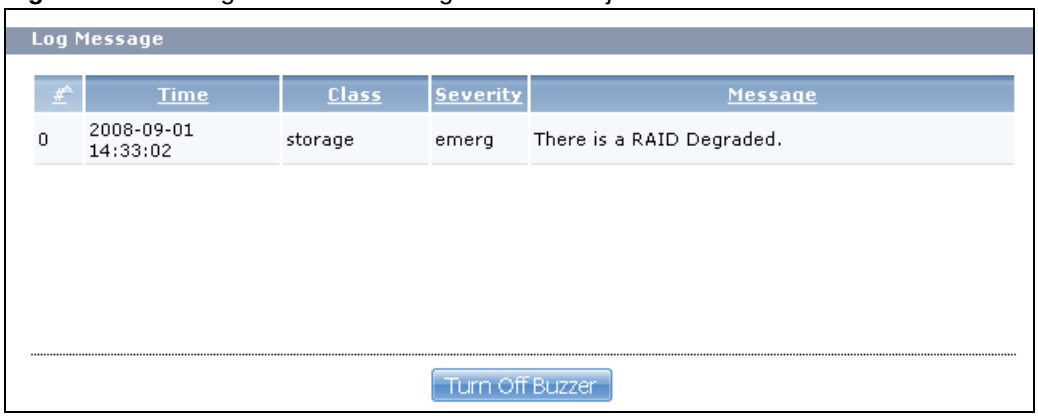
Figure 115 Storage > Internal Storage > Disk > Eject


Eject Disk
Are you sure to eject the disks?
Performing this operation will cause some network services to temporarily disconnect.
Apply
Cancel

3 Remove the hard drive. The NSA sounds an audible alarm.

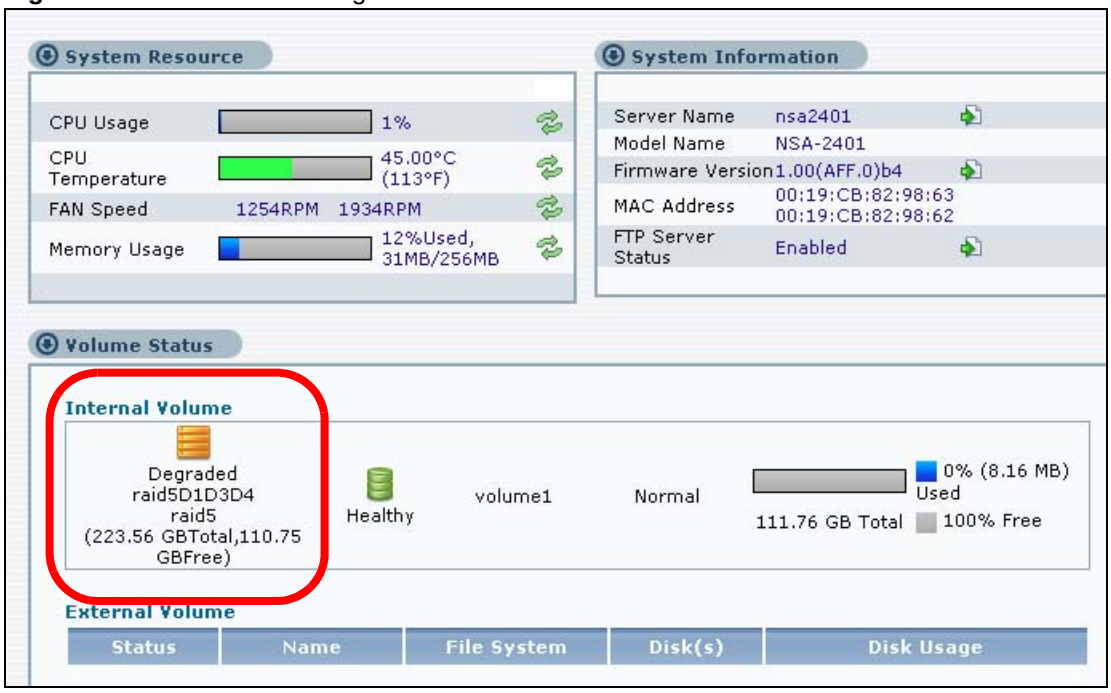
4 Log out of the Web Configurator and then back in. The **Log Message** screen shows that the RAID is degraded, click **Turn Off Buzzer** to stop the audible alarm. Then click **OK** to continue.

Figure 116 Storage > Internal Storage > Disk > Eject



5 Open the administration screens. In the **Status** screen the RAID array shows up as degraded.

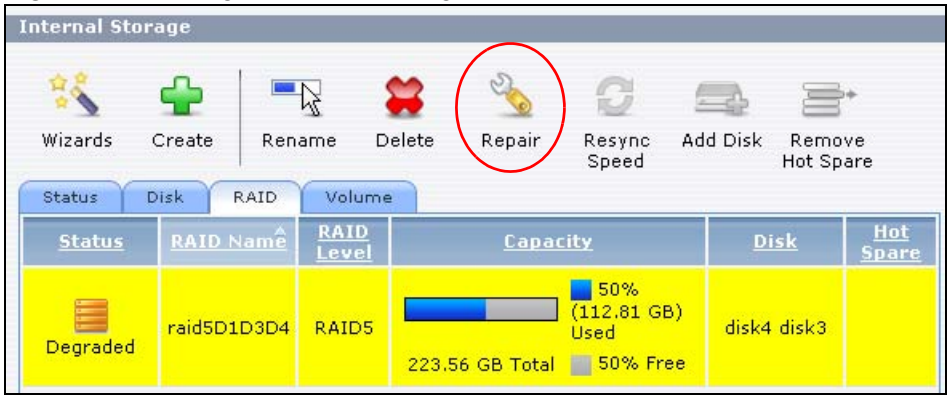
Figure 117 Status: RAID Degraded



6 Install the new hard drive. In this example it's in disk drive bay 2.

7 The NSA automatically repairs a degraded RAID if you insert an empty disk without an existing file system. Otherwise, after you insert a disk you must go to the **Storage** > **Internal Storage** > **RAID** screen and click **Repair**.

Figure 118 Storage > Internal Storage > RAID

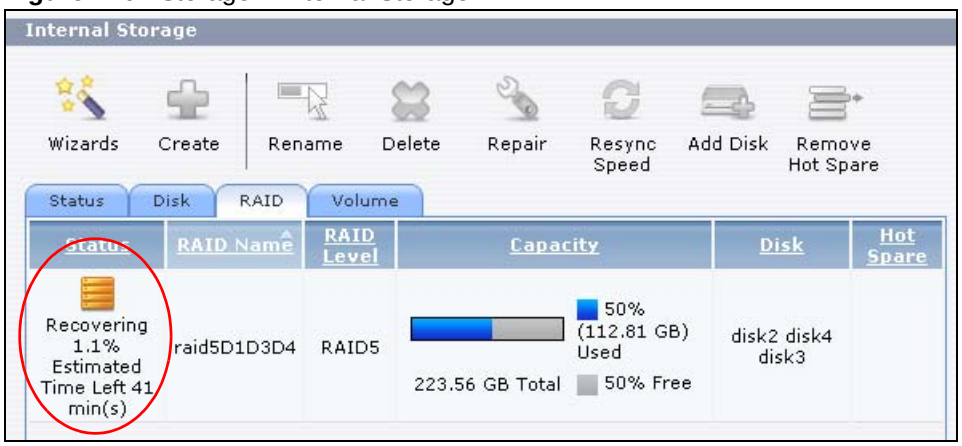


8 Select the disk you want to use to repair the RAID and click **Apply**.

Figure 119 Storage > Internal Storage > RAID > Repair

9 The RAID's status displays as **Recovering**.

Figure 120 Storage > Internal Storage > RAID



After the recovery finishes and the status shows up as **Healthy**, reboot the NSA. Then you can use the same process to migrate any (or all) of the RAID's drive as long as you replace them one-by-one and recover the RAID after each replacement. When you are done replacing hard drives and the final RAID recovery finishes, you can assign the increased storage capacity to your existing volumes (see Section 3.9.3 on page 109).

PART II
Web Configurator

Status Screen (117)
System Setting Screen (121)
Storage Screens (125)
Network Screens (159)
Sharing Screens (173)
Protect Screens (197)
Application Screens (223)
Maintenance Screens (229)

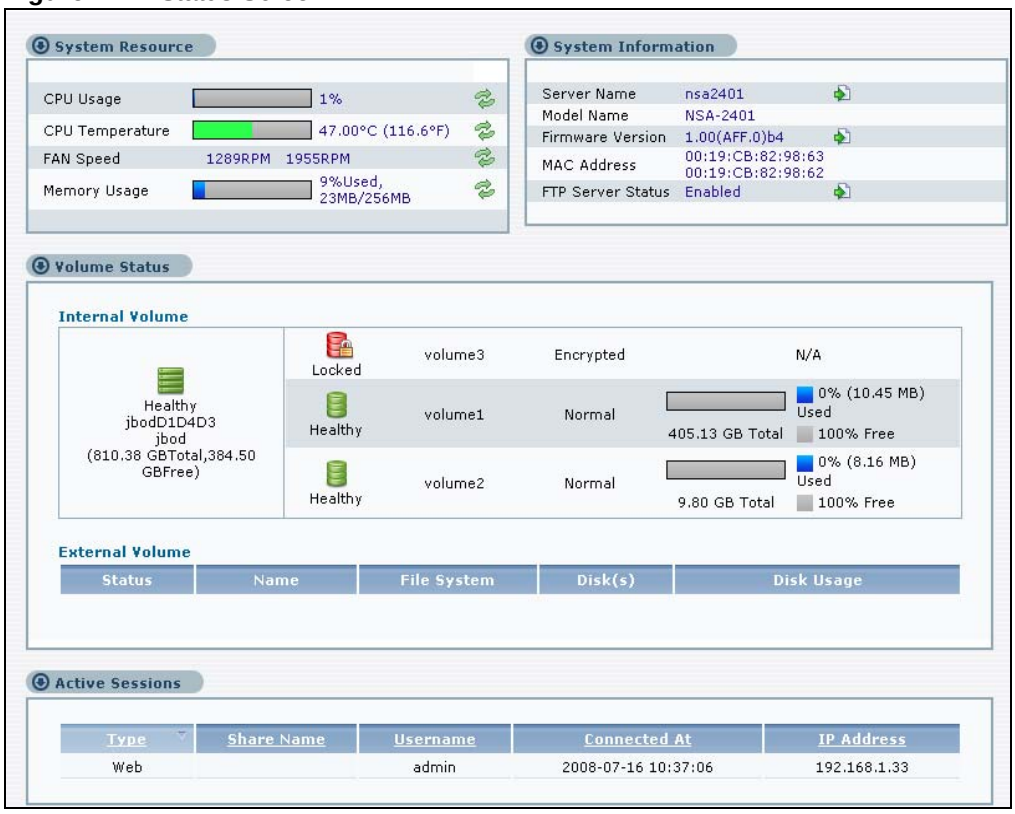
4

Status Screen

4.1 Status Screen

The **Status** screen is the first screen you see after you log into the Web Configurator (and complete the wizard for the first time). It provides an overview of your NSA's status, settings and activity. Once you leave the screen, you can return to it by clicking the **Status** icon or the text itself on the top-left of the navigation panel.

Figure 121 Status Screen


System Resource
CPU Usage 1%
CPU Temperature 47.00°C (116.6°F)
FAN Speed 1289RPM 1955RPM
Memory Usage 9%Used, 23MB/256MB
System Information
Server Name nsa2401
Model Name NSA-2401
Firmware Version 1.00(AFF.0)b4
MAC Address 00:19:CB:82:98:63 00:19:CB:82:98:62
FTP Server Status Enabled
Volume Status
Internal Volume
Healthy jbodD1D4D3 jbod (810.38 GBTotal,384.50 GBFree)
Locked volume3 Encrypted N/A
Healthy volume1 Normal 405.13 GB Total 0% (10.45 MB) Used 100% Free
Healthy volume2 Normal 9.80 GB Total 0% (8.16 MB) Used 100% Free
External Volume
Status Name File System Disk(s) Disk Usage
Active Sessions
Type Share Name Username Connected At IP Address
Web admin 2008-07-16 10:37:06 192.168.1.33

The following table describes the icons in this screen.

Table 16 Status Icons

ICON	DESCRIPTION
	Refresh Click this icon to refresh the data for the field or value with which it is associated.
	Edit Click this icon to open the configuration screen for the item with which it is associated.
	Healthy Green indicates a healthy disk array. All disks in the array are OK and the file system is functioning properly.
	Resynching Yellow indicates the raid array is being repaired or created.
	Waiting to Resync Indicates that another array is already being resynchronized. Only one array can resynchronize at a time.
	Degraded Indicates that a disk array is currently down, but can be fixed. Data access may be slower from a degraded array, so it's recommended that you replace the faulty disk and repair the array as soon as you can.
	Down Indicates that a disk array is down and cannot be fixed
	Healthy Green indicates a healthy volume. The volume is OK and the file system is functioning properly.
	Locked Volume Indicates that the volume has been locked with encryption. The password is set the first time the volume is locked.
	Unlocked Volume Indicates that the volume has an encryption layer than can be activated on the fly. The first time you lock a volume this encryption layer is created.
	Down Indicates that a volume is down and can not be fixed

The following table describes the labels in this screen.

Table 17 Status

LABEL	DESCRIPTION
System Resources	
CPU Usage	This displays a summary of CPU usage by all current processes. Click the **Refresh** icon to update this display. It also automatically updates itself every 10 seconds. Note: If too many users are using the NSA then the NSA may appear sluggish.

Table 17 Status (continued)

LABEL	DESCRIPTION
CPU Temperature	This displays the current temperature near the NSA's CPU. The NSA generates an emergency log if the temperature goes out of the normal operating range. If the temperature goes even higher, the NSA shuts down automatically to avoid damage from overheating. If the NSA overheats, make sure the fans are working and it is in a well ventilated place. Click the **Refresh** icon to update this display. It also automatically updates itself every 60 seconds.
Fan Speed	This is the RPM (Rotations Per Minute) of the NSA's fans. Click the **Refresh** icon to update this display. It also automatically updates itself every 60 seconds.
Memory Usage	This shows how much of the NSA's total memory is being used. Click the **Refresh** icon to update this display. It also automatically updates itself every 10 seconds.
UPS Status	When you use an APC Uninterruptible Power Supply (UPS) with a USB connection to the NSA, this field displays the remaining charge for the UPS's battery. A UPS is advisable to protect sensitive data stored on the NSA in the event of a power outage. The NSA uses power from the UPS when the normal power source is down and while the UPS still has battery power. The NSA shuts itself down if the UPS's battery charge gets down to the percentage you specify in the Power Management screen (see Section 11.6 on page 242). This allows the NSA to shut down properly and avoid data loss caused by a power failure when the UPS stops supplying power. The NSA uses power from the normal power source again when its power returns. The APC UPS battery is recharged then too.
System Information	
Server Name	This displays the name which helps you find the NSA on the network. Click the **Edit** icon to go to the **Network > Windows/CIFS** screen where you can change the **Server Name**.
Model Name	This displays the device's model name.
Firmware Version	This is the NSA firmware version and the date created. Click the **Update** link to go to the **Maintenance > FW Upgrade** screen where you can upload new firmware.
MAC Address	This displays the unique network adapter Media Access Control numbers of the NSA's Ethernet ports. Every device on your network has a different MAC address.
FTP Server Status	This lets you know whether the FTP server is enabled or disabled. Click the **Edit** icon to go to the **Applications > FTP** screen where you can change your FTP settings.
Volume Status	
Internal Volume	This displays the disk arrays and volumes created on the hard drives installed in the NSA. The first icon represents a disk array. The text below the icon shows the array's status (**Healthy, Resynching, Degraded** or **Down**), followed by it's name, type, total storage capacity, and free storage capacity. The second column of icons represents the storage volumes on the array. The text below the icon shows the volume's status (**Healthy, Locked, Unlocked**, or **Down**). The following columns display the volume's name, whether the volume is encrypted (**CRYPTO**) or not (**NORMAL**), the total size of the volume, how much is currently in use, and how much is still available.

Table 17 Status (continued)

LABEL	DESCRIPTION
External Volume	This displays the volumes created on USB hard drives connected to the NSA. USB ports are numbered in the order that you connect USB devices.
Status	This shows whether the external (USB) volume is **Healthy, Locked, Unlocked,** or **Down**.
Name	This shows the NSA-generated name for an external (USB) volume.
File System	This field displays the type of file system that an external (USB) volume is using.
Disk(s)	This shows what type of data storage system the external (USB) volume has. It may show **REGULAR** or **OK** meaning that the NSA can read the volume but that it wasn't created by the NSA.
Disk Usage	This shows total disk size, the percentage of the external (USB) volume being used and the percentage that is available.
Active Sessions	
Type	This shows whether it's a Windows/CIFS or FTP connection to the NSA.
Share Name	This displays the shared folder name on the NSA that the user is connected to for CIFS sessions and is blank for FTP sessions.
Username	This displays the name of the user connected to the NSA if one is defined and **ANONYMOUS FTP** otherwise.
Connected At	This displays the date and time the user last connected to the NSA in year-day-month hour:minute:second, format.
IP Address	This displays the IP address of the computer connected to the NSA.

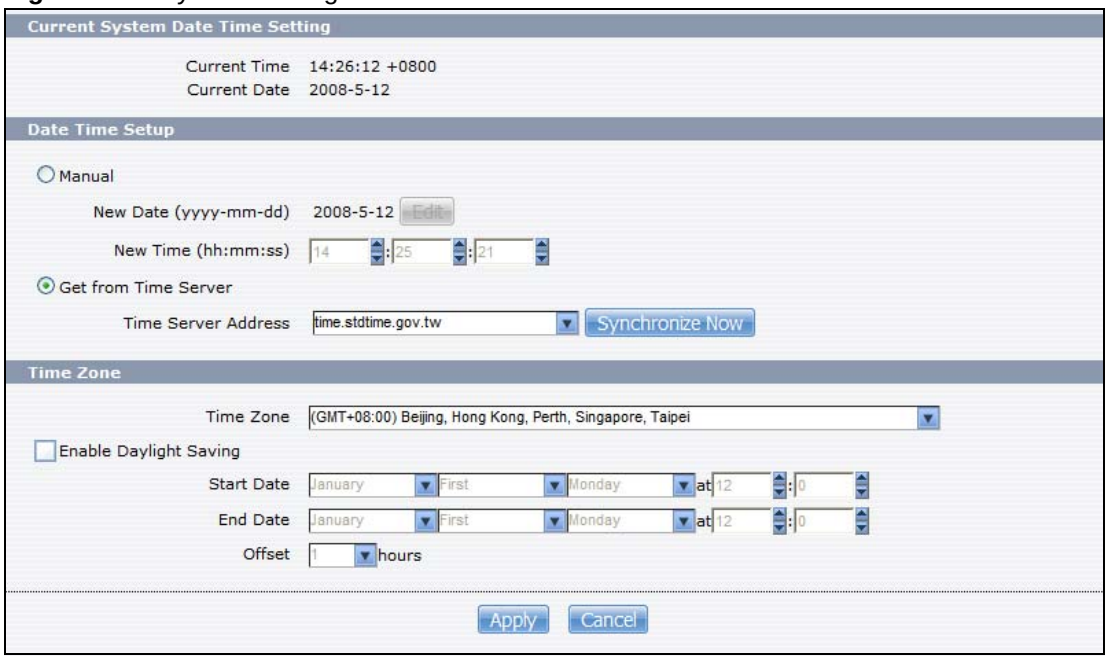
5

System Setting Screen

5.1 Date/Time

Use the NSA **System Setting** > **Date/Time** screen to set up the time on your NSA. To open this screen, click **System Setting** > **Date/Time** in the navigation bar of the Web Configurator. Choose a time zone and/or allow the NSA to synchronize with a time server.

Figure 122 System Setting > Date/Time


Current System Date Time Setting
Current Time 14:26:12 +0800
Current Date 2008-5-12
Date Time Setup
Manual
New Date (yyyy-mm-dd) 2008-5-12 Edit
New Time (hh:mm:ss) 14 : 25 : 21
Get from Time Server
Time Server Address time.stdtime.gov.tw Synchronize Now
Time Zone
Time Zone (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei
Enable Daylight Saving
Start Date January First Monday at 12 : 0
End Date January First Monday at 12 : 0
Offset 1 hours
Apply Cancel

The following table describes the labels in this screen.

Table 18 System Setting > Date/Time

LABEL	DESCRIPTION
Current Time	This field displays the time according to the NSA.
Current Date	This field displays the date according to the NSA.
Manual	Select this radio button to enter the time and date manually. When you enter the time settings manually, the NSA uses the new setting once you click **Apply**.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Date Time Setup** to **Manual**, enter the new date in this field and then click **Apply**.

Table 18 System Setting > Date/Time (continued)

LABEL	DESCRIPTION
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Date Time Setup** to **Manual**, enter the new time in this field and then click **Apply**.
Get from Time Server	Select this to have the NSA get the time and date from the time server you select in the **Time Server Address** field.
Time Server Address	Select a time server from the drop-down list box. Check with your ISP/ network administrator if you are unsure of this information.
Synchronize Now	Click this button for the NSA to retrieve the correct time from the configured time server right away.
Time Zone	Choose the NSA's time zone.
Enable Daylight Saving	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to gain more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The hour field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would use **March, [Second Sunday]**, at **2**:**00**. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **March**, **[Last Sunday]**. The time you specify depends on your time zone. In Germany for instance, you would enter 2 AM because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **November**, **First**, **Sunday**, at **2**:**00**. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **October**, **Last**, **Sunday**. The time you specify depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Offset	Specify by how many hours to change the time for Daylight Saving Time.
Apply	Click this to save your changes.
Cancel	Click this to discard changes.

5.1.1 Time Lag

Time lag occurs when the time on the NSA falls behind the time on the time server. This may happen if:

- The time server is no longer reachable.
- The NSA is shut down often. The NSA internal battery keeps time when the NSA is shut down and this may cause possible variance.
- A power surge occurs.

The NSA gives no warning if time lag occurs. You should re-synchronize the time after a power surge or after you have shut down the NSA several times.

6

Storage Screens

6.1 Storage Screens Overview

Use the storage screens to work with disks, RAIDs, and volumes to manage the NSA's storage.

6.1.1 What You Can Do in the Storage Screens

- Use the **Internal Storage** screens (Section 6.2 on page 127 through Section 6.6.1 on page 142) to view and configure the NSA's installed disks, RAIDs, and volumes.
- Use the **External Storage** screens (Section 6.7 on page 145 through Section 6.8.1 on page 149) to view and configure USB-connected disks and volumes.

6.1.2 What You Need to Know About Storage

Disks

Disks are the physical storage drives you use with the NSA. Internal storage is the hard drives you install inside the NSA. External storage is USB-connected drives.

RAIDs

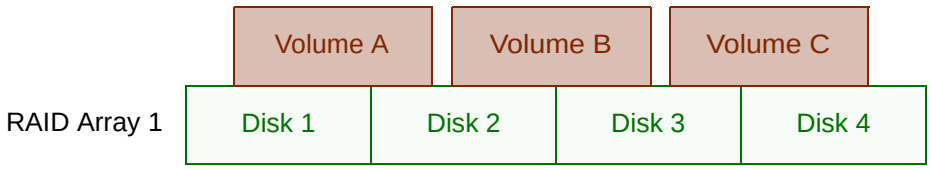
A hard drive array (RAID) is a storage method that lets you store data across multiple internal disks. You combine the internal disks into arrays. Each disk must belong to an array in order to use it. You can create multiple arrays.

Volumes

A volume is a storage area that you create on an array of internal disks or an external disk.

The following diagram shows disks one to four combined into **RAID Array 1**. Volumes **A**, **B**, and **C** are on **RAID Array 1**.

Figure 123 Disks, RAIDs, and Volumes



Encrypted Volumes

When you create a volume you can encrypt it using either a manually entered password or a USB key. Others cannot read the data even if they take the physical drive. Encrypting a volume does not affect how the volume's users use it. The NSA automatically encrypts data the users write to the encrypted volume and de-crypts the data they read.

Keep an encrypted volume's password or USB key in a safe place. Without the password or USB key, you cannot access the volume if it becomes locked. All of the volume's data will be unusable.

Locked and Unlocked Volumes

Keep an encrypted volume unlocked to allows users to use its shares as normal. Lock an encrypted volume to block all user access to its shares. The NSA automatically locks an encrypted volume if the disk is removed or the NSA restarts, is reset (since a reset includes a restart), or loses power. The administrator can also manually lock the volume. Once a volume is locked, no one can use it until an administrator unlocks it. The NSA does not take snapshots of a locked volume. See Chapter 9 on page 197 for more on snapshots.

Degraded Arrays

A degraded array is one that is damaged by a hard drive failure but can still be repaired by replacing the failed drive. The array is still operational but at risk since all of the array's data may be lost if a second hard drive fails. Data access may also be slower from a degraded array. It's recommended that you replace the faulty disk and repair the array as soon as you can.

The NSA automatically repairs a degraded RAID if you insert an empty disk without an existing file system. Otherwise, when you replace a disk you must go to the **Storage > Internal Storage > RAID** screen and click **Repair**.

Down Arrays

When an array is down, it cannot be fixed. The array cannot be used and the data is lost. Replace the faulty disk(s) and recreate the array, volumes, and sharing configuration.

Finding Out More

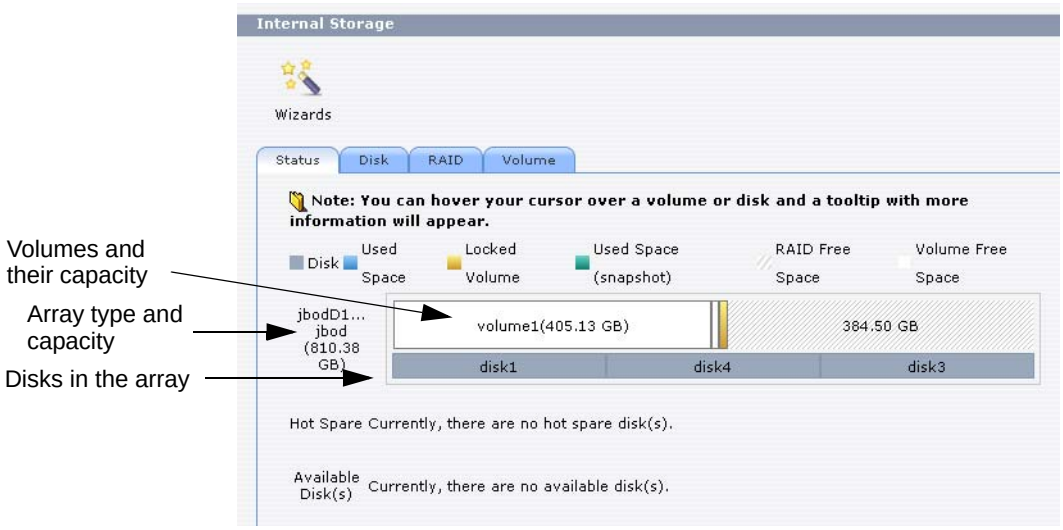
See Section 6.9 on page 151 for theoretical background information on JBOD and the RAID levels used on the NSA.

Read Section 3.9 on page 106 for how to increase the NSA's storage capacity.

6.2 Internal Storage Status Screen

Click **Storage** > **Internal Storage** > **Status** to display the following screen. This screen displays general information about the disks installed in the NSA and the disk arrays and volumes created on them.

Figure 124 Storage > Internal Storage > Status



The following table describes this screen.

Table 19 Storage > Internal Storage > Status

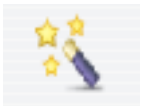
LABEL/ICON	DESCRIPTION
	**Wizards** Click this icon to open the **Disk Setup Wizard** to create a new disk array or volume.
Array type and capacity	The type of disk array (JBOD or RAID level) is listed first along with the array's capacity. See Section 6.4 on page 132 for more on the types of disk array.
Volumes and their capacity	The name and capacity of each volume in the array.
Disk	This represents the internal (physical) hard drives.
Used Space	This represents how much of a volume's capacity is currently filled by files.
Locked Volume	This represents a volume to which the NSA is blocking access.
Used Space (snapshot)	Snapshots (records of changes to files within a volume) are stored in the space on the disk array that is not allocated to volumes. This represents how much of that space is currently filled by snapshots. See Chapter 9 on page 197 for more on snapshots.
RAID Free Space	This is space on the disk array that is not allocated to volumes and is not (yet) used by snapshots.
Volume Free Space	This is space on a storage volume that is not used up by files.
Disks in the array	The disks that belong to the array display under the array's volumes.

Table 19 Storage > Internal Storage > Status (continued)

LABEL/ICON	DESCRIPTION
Hot-Spare	This is the array's standby drive if it has one. "There are not disks" displays if the array does not have a standby drive.
Free	These are installed disks that do not already belong to a disk array.

6.3 Disk

You can view information on the NSA internal disks in this screen.

Disk Replacement Restrictions

See the Quick Start Guide for information on replacing disks in the NSA. When replacing a disk in a degraded or down RAID array, the new disk must be at least the same size or bigger than the array's smallest disk, so the NSA can restore all data in the array. For optimal performance, all disks in the array should be the same model, capacity, and speed.

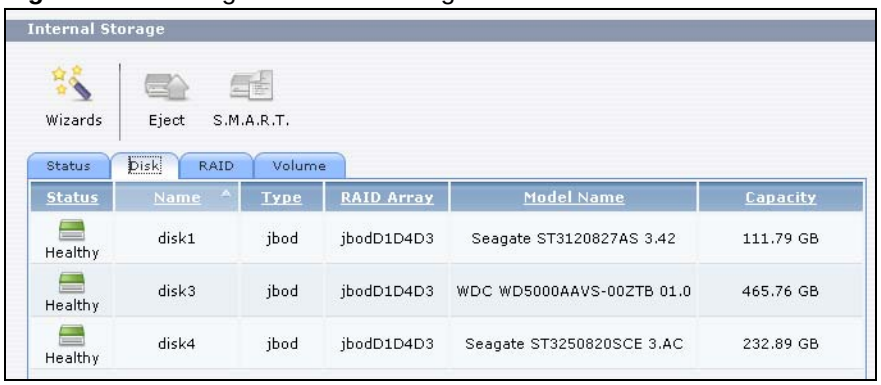
For example, if you have RAID with 250 GB disks, you must put in a 250 GB or bigger disk as a replacement in order to restore all original data in that array. If you use a bigger disk, the extra space on the disk will not be used.

The NSA automatically repairs a degraded RAID if you insert an empty disk without an existing file system. Otherwise, when you replace a disk you must go to the **Storage > Internal Storage > RAID** screen, select the degraded array, and click **Repair**.

6.3.1 Internal Disks Screen

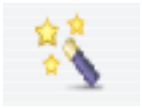
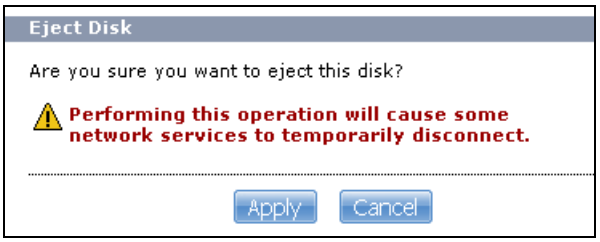
Click **Storage** > **Internal Storage** > **Disk** to display the following screen. This screen provides information on disks installed in the NSA.

Figure 125 Storage > Internal Storage > Disk



The following table describes the icons in this screen.

Table 20 Storage > Internal Storage > Disk Icons

ICON	DESCRIPTION
	**Wizards** Click this icon to open the **Disk Setup Wizard** to create a new disk array or volume.
	Eject Select a hard drive and click this icon to shut it down. Do this before removing a hard drive to help increase its usable lifetime. Note: Ejecting a disk from a JBOD or RAID0 array causes the array to fail and the data to be lost. 
	S.M.A.R.T. Select a hard drive and click this icon to display details about the drive and its status. The S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) monitoring system detects and reports on hard drive reliability indicators to help anticipate failures. This feature can be useful for troubleshooting.
	Sort Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.
	Status This icon shows if the hard disk is functioning normally.

The following table describes the labels in this screen.

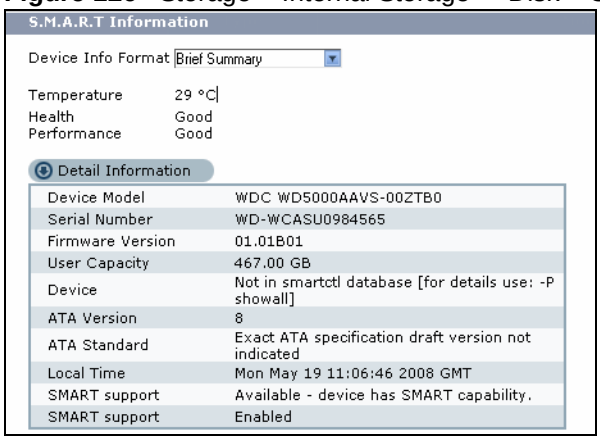
Table 21 Storage > Internal Storage > Disk

LABEL	DESCRIPTION
Name	This field shows **disk1**, **disk2**, **disk3**, and/or **disk4** for disks installed in the NSA disk trays labelled 1, 2, 3 and 4 respectively.
Type	This shows the kind of array to which the disk belongs. See Section 6.4 on page 132 for details.
Model Name	This is the hard drive model number that uniquely identifies a hard drive.
Capacity	This field shows the size of the hard disk.

6.3.2 S.M.A.R.T Screen

Click **Storage** > **Internal Storage** > **Disk** to display the disk summary screen. Select a disk and click the **S.M.A.R.T**. icon to display the following screen. This screen provides details about the drive and its status.

Figure 126 Storage > Internal Storage > Disk > S.M.A.R.T. (Brief Summary)


S.M.A.R.T Information
Device Info Format Brief Summary
Temperature 29 °C
Health Good
Performance Good
Detail Information
Device Model WDC WD5000AAVS-00ZTB0
Serial Number WD-WCASU0984565
Firmware Version 01.01B01
User Capacity 467.00 GB
Device Not in smartctl database [for details use: -P showall]
ATA Version 8
ATA Standard Exact ATA specification draft version not indicated
Local Time Mon May 19 11:06:46 2008 GMT
SMART support Available - device has SMART capability.
SMART support Enabled

The following table describes this screen.

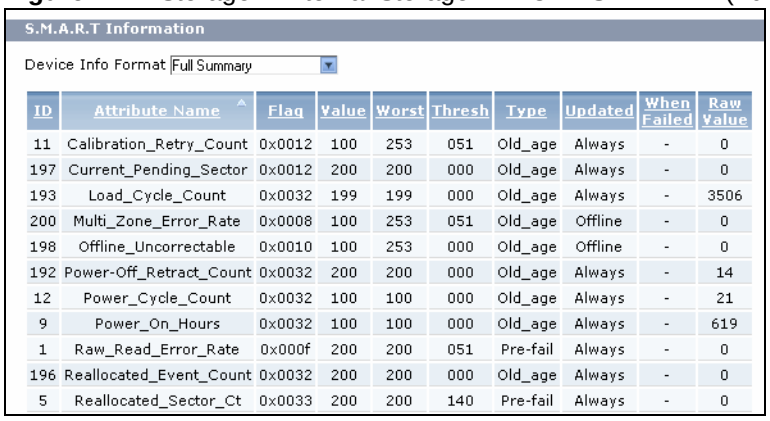
Table 22 Storage > Internal Storage > Disk > S.M.A.R.T. (Brief Summary)

LABEL/ICON	DESCRIPTION
Device Info Format	Select **Brief Summary** to display basic information about the drive and its status. Select **Full Summary** to display advanced details about the drive and its status.
Temperature	This field displays the hard drive's temperature in degrees Celsius.
Health	This field displays a general rating of the hard drive's overall operating condition.
Performance	This field displays a general rating of the hard drive's overall operating speed.
Detail Information	These fields tell you details about the hard drive, such as identification information. They are not indicators of the hard drive's health or performance.
Device Model	This field displays the hard drive model number that uniquely identifies a hard drive.
Serial Number	This field displays this individual hard drive's serial number from the manufacturer.
Firmware Version	This field displays the version number of the hard drive's internal operating software.
User Capacity	This field displays the hard disk's usable size.
Device	This field displays whether or not the hard drive is in the Control and Monitor Utility for SMART disks database.
ATA Version	This field displays the hard disk's Advanced Technology Attachment version number.
ATA Standard	This field displays the Advanced Technology Attachment standard the hard drive supports.
Local Time	This field displays the local time that the hard drive is using.
SMART support	This field displays whether or not the hard drive is SMART-capable.
SMART support	This field displays whether or not the hard drive has SMART monitoring turned on.
OK	Click this button to close the screen.

6.3.2.1 S.M.A.R.T Full Summary

Set the **Device Info Format** field to **Full Summary** to display advanced details about the drive and its status. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 127 Storage > Internal Storage > Disk > S.M.A.R.T. (Full Summary)


S.M.A.R.T Information

Device Info Format: Full Summary

ID	Attribute Name	Flag	Value	Worst	Thresh	Type	Updated	When Failed	Raw Value
11	Calibration_Retry_Count	0x0012	100	253	051	Old_age	Always	-	0
197	Current_Pending_Sector	0x0012	200	200	000	Old_age	Always	-	0
193	Load_Cycle_Count	0x0032	199	199	000	Old_age	Always	-	3506
200	Multi_Zone_Error_Rate	0x0008	100	253	051	Old_age	Offline	-	0
198	Offline_Uncorrectable	0x0010	100	253	000	Old_age	Offline	-	0
192	Power-Off_Retract_Count	0x0032	200	200	000	Old_age	Always	-	14
12	Power_Cycle_Count	0x0032	100	100	000	Old_age	Always	-	21
9	Power_On_Hours	0x0032	100	100	000	Old_age	Always	-	619
1	Raw_Read_Error_Rate	0x000f	200	200	051	Pre-fail	Always	-	0
196	Reallocated_Event_Count	0x0032	200	200	000	Old_age	Always	-	0
5	Reallocated_Sector_Ct	0x0033	200	200	140	Pre-fail	Always	-	0

The following table describes this screen.

Table 23 Storage > Internal Storage > Disk > S.M.A.R.T. (Full Summary)

LABEL/ICON	DESCRIPTION
Device Info Format	Select **Brief Summary** to display basic information about the drive and its status. Select **Full Summary** to display advanced details about the drive and its status.
ID	This field displays the identifier number of the S.M.A.R.T. attribute.
Attribute Name	This field displays the text name of the S.M.A.R.T. attribute. See Section 6.9.9 on page 156 for a list of common S.M.A.R.T. attributes.
Flag	This field displays the S.M.A.R.T. attribute's flag.
Value	This is the attribute's current (or most recent) normalized value. These normalized values range from 1 to 254 and are almost always mapped so higher values are better. Compare this with the threshold value.
Worst	This is the hard drive's worst recorded normalized value for this attribute. Compare this with the threshold value.
Thresh	This is the attribute's threshold value. If the attribute's current normalized value is less than or equal to the threshold, the attribute has failed. An attribute value close to or below the threshold indicates the hard drive is no longer reliable.
Type	Attributes can be one of two types: Pre-failure (**Pre-fail**) or Old age (**Old_age**). Pre-failure attributes are ones that indicate imminent hard drive failure if the attribute value is less than or equal to the threshold. Old age attributes indicate end-of-product life from old-age (normal wearing out) if the attribute value is less than or equal to the threshold. Note that just because an attribute is of the Pre-fail type does not mean your hard drive is ready to fail. If only means this if the current normalized value of the attribute is less than or equal to the threshold.
Updated	This indicates when the hard drive updates the value for this attribute. **Always** means the hard drive updates this attribute during normal operation and during offline activities. **Offline** means the hard drive only updates this attribute when no one is accessing the hard drive.

Table 23 Storage > Internal Storage > Disk > S.M.A.R.T. (Full Summary) (continued)

LABEL/ICON	DESCRIPTION
When Failed	This column indicates when (if ever) the attribute failed. An attribute has failed if the normalized value is less than or equal to the threshold. **-**: This displays if the attribute is not failing now and has never failed in the past. **FAILING_NOW**: This displays if the attribute's current normalized value is less than or equal to the threshold. **In_the_past**: This displays if the attribute's current normalized value is greater than the threshold but the worst recorded value is less than or equal to the threshold.
Raw Value	This is the attribute's unprocessed raw data. These values show exact amounts of time or numbers of attempts or errors. The meaning to the raw values is specific to the hard drive manufacturer. Table 42 on page 156 has some information about whether a higher or lower individual raw S.M.A.R.T. attribute value is better.
OK	Click this button to close the screen.

6.4 Arrays

RAID (Redundant Array of Independent Disks) or JBOD is the storage method that the NSA uses. The storage method you use depends on how many disks you have and how many volumes you want to create. It's important that you consider this carefully as all data is deleted when you re-create a volume.

RAID is a method of storing data on multiple disks to provide a combination of greater capacity, reliability, and/or speed. The NSA also supports JBOD (Just a Bunch Of Disks) which is not technically a RAID storage method. You combine multiple physical disks into a RAID or JBOD array.

Hard Drives to Use With RAID

You can use RAID or JBOD for the physical hard disk drives installed in the NSA's drive bays. If you use RAID (instead of JBOD), it is recommended that you use hard drives of the same storage capacity as RAID uses the capacity of the array's smallest drive. For example, if you have four disks of sizes 100 GB, 150 GB, 150 GB and 200 GB respectively in one RAID array, then the maximum capacity is based on the size of the smallest disk size (100 GB) and the remaining space (300 GB) is unused.

6.4.1 RAID Levels

The type of array you use depends on how many disks you have and how many arrays you want to create. Consider this carefully as all data is deleted when you re-create an array.

Back up your data before deleting or re-creating an array

For example if you originally have two disks configured in a RAID 1 array, and you then buy two more disks and want to configure all four at RAID 5, you should first back up all your data on those disks (see the Genie Backup Manager utility on the included CD) and then restore your data later after you create the new array.

Below is a table that summarizes some attributes of the various array levels as supported on the NSA. For capacity and storage efficiency, “S” is the size of the smallest drive in the array, and “N” is the number of drives in the array.

Performance rankings are approximations.

Table 24 RAID Array Levels Quick Comparison

Type of Array	RAID 0	RAID 1	RAID 5	RAID 10	JBOD
Number of Disks	2,3,4	2	3,4	4	1,2,3,4
Capacity	S*N	S*N/2	S*(N-1)	S*N/2	sum of disks
Storage Efficiency[A]	100%	50%	(N-1)/N	50%	100%
Fault Tolerance	None	YYYY	YYY	YYYY	Y
Availability	Y	YYYY	YYYY	YYYY	YY
Read Performance	YYYY	YYY	YYYY	YYYY	YY
Write Performance	YYYY	YYY	YY	YYY	YY

A. Storage efficiency means what percent of the possible storage capacity can be used. This table assumes all drives in a RAID array are of identical size. A JBOD array provides capacity equal to the sum of all disks in the array.

The following is a guide to help you choose a RAID level depending on how many disks you have installed in the NSA. See Section 6.9 on page 151 for technical background on JBOD and the RAID levels used on the NSA.

One Disk

With only one disk, you must use JBOD. All disk space is used for your data - none is used for backup. If the disk fails, then you lose all the data on that array. You can later add another disk to your one-disk JBOD array (without having to re-create shares, access rights and so on) or create a different JBOD array (and create new shares, access rights and so on).

Two Disks:

You may choose JBOD, RAID 0 or RAID 1. With two disks you could create:

- one or two JBOD arrays
  - JBOD gives flexibility and maximum disk space usage. You can later add another disk to your JBOD array (without having to re-create shares, access rights and so on) or create a different JBOD array (and create new shares, access rights and so on).
- one RAID 0 or RAID 1 array
  - RAID 0 offers higher performance but no data security. It has the fastest read and write performance since it reads and writes to both disks simultaneously, but if one disk fails you lose all your data in the array. Performance may matter more than data security to gamers for example. This method may also be acceptable for data that is already backed up somewhere else.
  - RAID 1 offers data security, although the performance is slower than RAID 0. Since RAID 1 mirrors data onto a second disk, you can recover all data if one disk fails.

Three Disks

Choose a combination of JBOD and/or RAID 0 or RAID 1 for the reasons already outlined. With three disks you could create:

- up to three JBOD arrays
- one RAID 1 array with a hot-spare.
- one single-disk JBOD array and one two-disk RAID 0 or one two-disk RAID 1 array
- one RAID 5 array

Four Disks

In addition to the JBOD, RAID 0 and RAID 1 choices, you may choose RAID 10, RAID 5 or RAID5_(3 + hot-spare). With four disks you could create:

- up to four JBOD arrays
- one or two JBOD arrays and one RAID 0 or RAID 1 array
- two RAID 0 arrays or two RAID 1 arrays
- one RAID 0 array and one RAID 1 array
- one RAID 5 array (with three disks) and one JBOD array
- one array using one of RAID 10, RAID 5 or RAID5_(3 + hot-spare)
  - RAID 10 (RAID 1 +0) offers maximum data security but just 50% of the storage space. RAID 10 (RAID 1+0) is a nested RAID where two RAID 1 arrays are stored on the physical disks with a RAID 0 array on top.You can recover all data even if two disks (not in the same RAID 1 array) fail. If two disks in the same RAID 1 array fail, then all data in the array is lost. If two disks in different RAID 1 arrays fail, then you effectively have a RAID 0 configuration.
  - RAID 5 provides more storage space and protection against up to one disk failure. RAID 5 uses 75% of the available space for your data. All data can be recovered if one disk fails. If two disks fail then, all data in the array is lost. If one disk fails, the array is degraded and will perform more slowly than a healthy array. You should replace the faulty disk and re-synchronize the array to attain previous performance.
  - RAID5 (with hot-spare) automatically recovers the array if a disk fails. It operates as a three-disk RAID 5 array with the fourth disk on standby. If a disk in the 3-disk RAID5 array fails, the NSA automatically uses the standby disk to re-synchronize the array so it gets back to operating at healthy array speed as quickly as possible. RAID5 (with hot-spare) uses 50% of the available space for your data.

6.4.2 Array Status

You (the administrator) can see the status of an array in the **Status**, or **Storage** > **Internal Storage** > **RAID** screens.

The NSA has the following classifications for the status of an array:

- **Healthy** if all disks in the array are OK and the file system is functioning properly.
- **Resynching** when you create or repair a RAID array.
- **Degraded** when an array is damaged (a hard drive has failed), but can be fixed. The array is still operational but at risk since all of the array's data may be lost if a second hard drive fails. Data access may be slower from a degraded array, so it's recommended that you replace the faulty disk and repair the array as soon as you can.

- **Down** when an array is down and cannot be fixed. The array cannot be used and the data is lost. Replace the faulty disk(s) and recreate the array, volumes, and sharing configuration.

If an array is down, users can no longer transfer files to/from the array's shares. If an array is degraded, then file transfer to/from the shares in the degraded array will be slower.

Although there is no explicit message from CIFS that tells users an array is degraded or down, you can have the NSA send the administrator an email alert.

Resynchronizing and Reshaping

The NSA resynchronizes a RAID 1, RAID 5, or RAID 10 array to repair it. When you add a disk to a three-disk RAID 5 array, the NSA reshapes it into a four-disk RAID 5 array. Resynchronizing or reshaping an array is done block-by-block, so the time it takes depends on the size of your hard drive(s), not the amount of data you have on them.

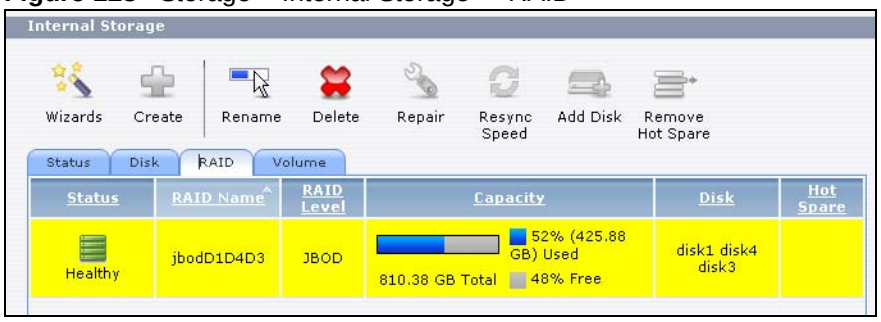
Do not restart the NSA while the NSA is re-sychronizing or reshaping an array as this will cause the process to start over from the beginning again after the NSA fully reboots.

You can access data on a RAID array while the NSA is re-sychronizing or reshaping it, but it is not recommended. The performance will be slower and your data is at risk until the resychronization or reshaping is complete.

6.5 RAID Screen

Click **Storage** > **Internal Storage** > **RAID** to display the RAID array summary screen as shown. Use this screen to manage the NSA RAID (and JBOD) arrays.

Figure 128 Storage > Internal Storage > RAID



The following table describes the icons in this screen.

Table 25 Storage > Internal Storage > RAID Icons

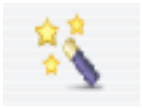
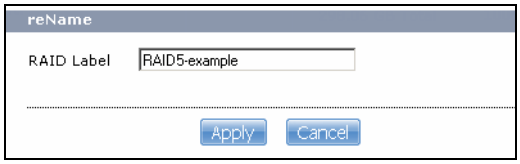
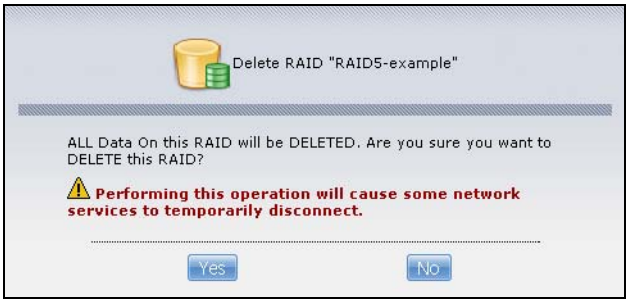
ICON	DESCRIPTION
	**Wizards** Click this icon to open the **Disk Setup Wizard** to create a new disk array or volume.
	Create If you have disk space available for a new disk array, then click this icon to open a screen where you can create a new disk array.
	Rename Select a hard drive array and click this icon to change the array's name. 
	Delete Select a hard drive array and click this icon to remove the array. You must remove all of an array's volumes before you can delete the array. Note: Deleting an array also deletes all data in the array's disk(s). A warning screen appears. Click **Yes** if you want to remove the array and all of its data. Otherwise click **No**. 
	Repair After you replace a faulty disk, select the hard drive array (its status will be **Degraded**) and click this icon to resynchronize the array.

Table 25 Storage > Internal Storage > RAID Icons (continued)

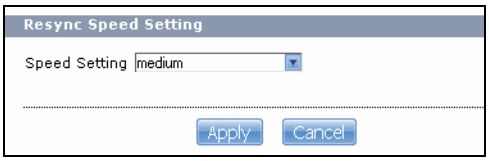
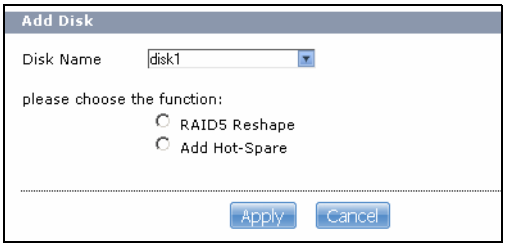
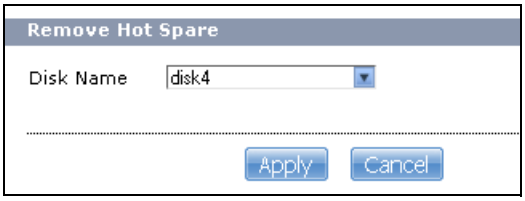
ICON	DESCRIPTION
	Resync Speed When a disk array is resynchronizing, you can select it and click this icon to set how fast the NSA resynchronizes the disk array. A screen displays.  Select the how fast the NSA should re-synchronize the array. The faster the resynchronization, the slower the performance for users accessing shares. With resynchronizing at a high priority, users may have limited access speed to shares until resynchronization finishes.
	Add Disk To add another disk to an existing JBOD, RAID1, or RAID5 array, select the array and click this icon. You can add a disk to increase an array's capacity or to use as a hot-spare (standby). When you add a disk to an existing array, you do not have to re-create shares, access rights and so on as you would if you created a new array.  **Reshape**: Make a three disk RAID5 array into a four disk RAID5 array. **Expand JBOD**: Add another disk to a JBOD array. **Add Hot-Spare**: Add a standby disk. For a RAID1 or RAID5 array, the capacity of the disk you are adding must be equal to or greater than the smallest disk in the array.
	Remove Hot Spare To remove the standby drive from a RAID1 or RAID5 array, select the array and click this icon. After you do this, you can create a single-disk JBOD array for the disk. 

Table 25 Storage > Internal Storage > RAID Icons (continued)

ICON	DESCRIPTION
	Sort Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.
	Status This icon shows **Healthy, Resynching, Degraded** or **Down**; see Section 6.4.2 on page 134. If an array is degraded, click the **Repair** icon after you have replaced the faulty disk.

The following table describes the labels in this screen.

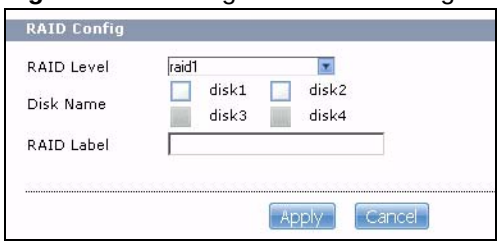
Table 26 Storage > Internal Storage > RAID

LABEL	DESCRIPTION
Label	This field shows the name of the array.
RAID Level	This field shows which type of data storage system (a RAID level or JBOD) the array is using. See Section 6.4 on page 132 for details on the different levels.
Capacity	This field shows the total size of the array, how much is currently in use, and how much is still available.
Disk	This field shows the hard disks that are in the array.
Hot Spare	If the array has a standby disk, this field identifies it.

6.5.1 Creating a New RAID

Click the **Create** icon in the **RAID** screen as shown in Figure 128 on page 135 to create a new RAID array.

Figure 129 Storage > Internal Storage > RAID > Create



The following table describes this screen.

Table 27 Storage > Internal Storage > RAID > Create

LABEL	DESCRIPTION
RAID Level	Use **JBOD** or **RAID 0** if you want maximum capacity and/or maximum speed for your disks, and/or you have other means of protecting your data. Use **RAID 1** to mirror primary data to another disk(s) with high performance. Use **RAID 5** with three disks to balance performance, hard disk capacity usage with data protection in case of disk failure. Use **RAID 10**, or **RAID 5** with four disks to balance performance, hard disk capacity usage with data protection in case of disk failure. See Section 6.4 on page 132 and Section 6.9 on page 151 for more information on storage systems.
Disk Name	Select which disks should make up this RAID array. A disk can only belong to one RAID array.
RAID Label	Specify a name to identify the RAID array. Use 1 to 31 characters. To avoid confusion, it is highly recommended that each RAID use a unique name. Acceptable characters are all alphanumeric characters (A-Z 0-9) and " " [spaces], “-” [dashes], "_" [underscores], and "." [periods]. The first character must be alphanumeric. The last character cannot be a space " ".
Apply	Click this button to save your changes back to the NSA.
Cancel	Click this button to discard your changes and close this screen.

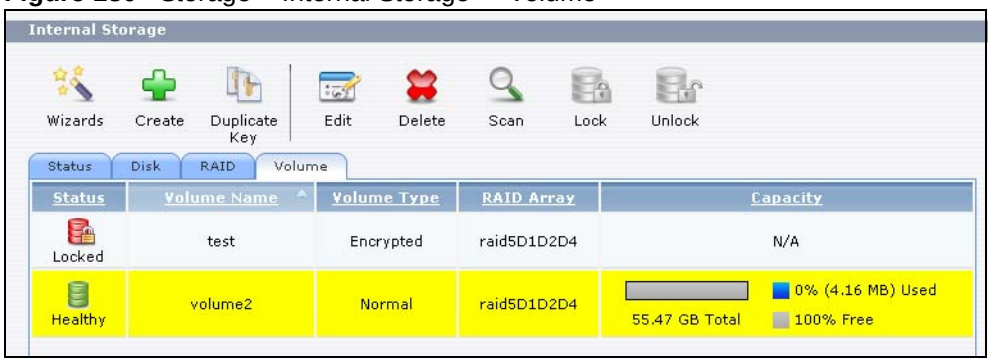
6.6 Internal Volume Screen

Click **Storage** > **Internal Storage** > **Volume** to display the internal volume summary screen as shown. Use this screen to manage the NSA’s internal volumes.

The NSA has the following classifications for the status of a volume:

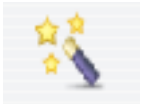
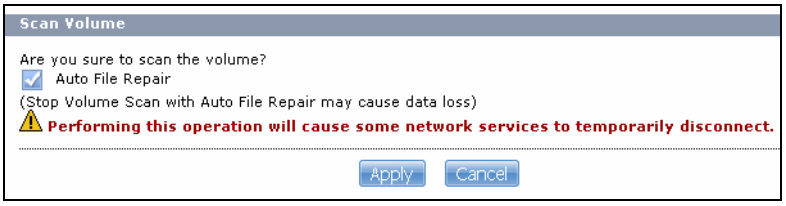
- **Healthy** if the volume is OK and the file system is functioning properly.
- **Unlocked** when the NSA allows access to an encrypted volume.
- **Locked** when the NSA blocks access to an encrypted volume. When a volume is locked, you (the administrator) can enter the password or insert the USB key (whichever you used to encrypt it) to unlock the volume.
- **Down** when a volume is down and cannot be fixed. The volume cannot be used and the data is lost. Replace the faulty disk(s) and recreate the array, volumes, and sharing configuration.

Figure 130 Storage > Internal Storage > Volume



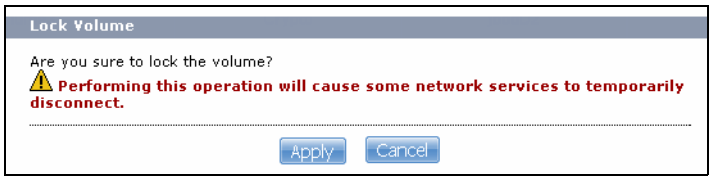
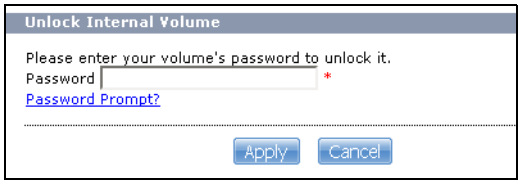
The following table describes the icons in this screen.

Table 28 Storage > Internal Storage > Volume Icons

ICON	DESCRIPTION
	**Wizards** Click this icon to open the **Disk Setup Wizard** to create a new disk array or volume.
	Create Click this icon to open a screen where you can create a new storage volume.
	Duplicate Key If you have volumes that were encrypted using a USB key, you can click this to go to the external volume screen where you can copy the USB key to a second USB device.
	Edit Select a volume and click this icon to modify it's settings.
	Delete Select a volume(s) and click this icon to remove the volume(s). Note: If you remove a volume, all data in the volume disk(s) is lost.
	Scan Select a volume and click this icon to check the volume's file consistency.  Note: If you have the NSA automatically attempt to repair any damaged files it finds during the scan, be careful not to cancel the scan as you may lose data.

Scan Volume
Are you sure to scan the volume?
Auto File Repair
(Stop Volume Scan with Auto File Repair may cause data loss)
Performing this operation will cause some network services to temporarily disconnect.
Apply
Cancel

Table 28 Storage > Internal Storage > Volume Icons (continued)

ICON	DESCRIPTION
	Lock If an encrypted volume is unlocked, you can select it and click this icon to lock it. No one will be able to use the volume until an administrator unlocks it. Note: At start up, if a USB key is inserted, the NSA automatically unlocks any volumes encrypted by the USB key. 
	Unlock The NSA automatically locks an encrypted volume if the NSA loses power or the disk is removed. Select a locked volume and click this icon to open a screen where you can enter the volume's password or use the USB key to allow users to use the volume again. If you forgot the password, click **Password Prompt** to display the hint you configured to help you remember it.  If the USB device containing the volume's key is already inserted, remove it and re-insert it.
	Sort Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.
	Status This icon shows whether the volume is **Healthy, Locked, Unlocked,** or **Down**.

The following table describes the labels in this screen.

Table 29 Storage > Internal Storage > Volume

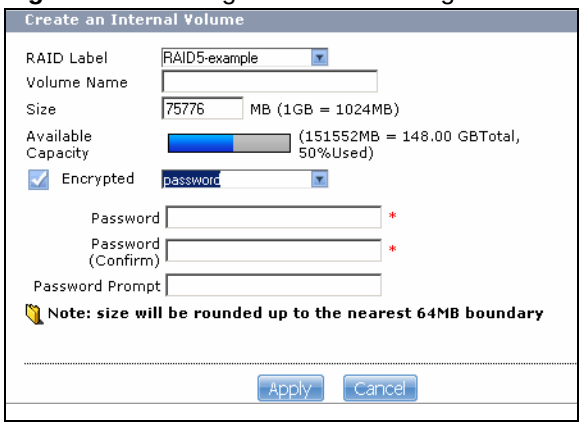
LABEL	DESCRIPTION
Volume Name	This field shows the name of the volume.
Volume Type	This field shows the volume is unencrypted (**Normal**) or encrypted (**Crypto**).
RAID Array	This field shows the RAID or JBOD array on which the volume is located.
Capacity	This field shows the total size of the volume, how much is currently in use, and how much is still available.

6.6.1 Creating or Editing an Internal Volume

Click **Storage** > **Internal Storage** > **Volume** > **Create** to display the internal volume creation screen as shown next. You can also select an existing internal volume and click the **Edit** icon. Use this screen to add or edit internal storage volumes.

Keep an encrypted volume's password or USB key in a safe place. You cannot access a locked volume without the password or USB key. All of the volume's data will be unusable. If you use a USB key, keep backup copies. Do not use the USB key for anything else (do not store data on it or format it).

Figure 131 Storage > Internal Storage > Volume > Create



The following table describes this screen.

Table 30 Storage > Internal Storage > Volume Create

LABEL	DESCRIPTION
RAID Label	Select the disk array upon which you want to create the volume. This option is only available when you create a volume.
Volume Name	Type a volume name from 1 to 31 characters. To avoid confusion, it is highly recommended that each volume use a unique name. Acceptable characters are all alphanumeric characters (A-Z 0-9) and " " [spaces], "-" [dashes], "_" [underscores], and "." [periods]. The first character must be alphanumeric. The last character cannot be a space " ".
Size	Enter the number of megabytes to use for the volume. Click the screen to update the **Available Capacity** display. You can edit a volume later to make it larger (but not smaller). You may want to leave some capacity on the array un-allocated to volumes since the NSA uses that space to store snapshots. So the bigger the volumes are, the less space there is for snapshots. See Chapter 9 on page 197 for more on snapshots.
Available Capacity	This field shows the total storage space available on the array and how much of it this volume will take up.

Table 30 Storage > Internal Storage > Volume Create (continued)

LABEL	DESCRIPTION
Encrypted	Select this check box and an option from the drop-down list box to encrypt the volume. This option is only available when you create a volume. The NSA automatically locks an encrypted volume if the NSA restarts or loses power or the disk is removed. An administrator can also manually lock the volume. Once a volume is locked, no one can use it again until an administrator unlocks it. Encryption affects the NSA's write speeds. **password**: Select this option to manually enter a password for the volume. You can also enter a password prompt hint to help you remember the password if you forget it. You will need to manually re-enter the key every time the NSA restarts. **USB key**: Select this option to have the NSA create a password for the volume and store the password on a connected USB device. Later, if the volume is locked, the NSA automatically unlocks it when you insert the USB key. At start up, if a USB key is inserted, the NSA automatically unlocks any volumes encrypted by it.
Password	The password fields display if you choose to encrypt the volume by manually entering a password. Enter a password for encrypting the volume.
Password (Confirm)	Re-type the password to make sure you entered it correctly.
Password Prompt	Enter a hint to help you recall the password if you forget it.
USB Key	The USB field and button display if you choose to encrypt the volume by USB key. Select a USB key device that you created previously or select a USB device that you want to make into a USB key. If the USB device is not already connected, connect it and click the **Refresh** icon. The NSA's upper USB port is **USB1** and its lower USB port is **USB2**. It is recommended that you use a USB device to store a volume key only and not also use it for storage.
Create USB Drive	Click this button to go to screens you can use to create a password for unlocking the volume and store the password on a connected USB device. You also use the screens to create copies of the USB key. Note: Create duplicate USB keys now since you cannot make them later.
Apply	Click this button to create the volume.
Cancel	Click this button to discard your changes and close this screen.

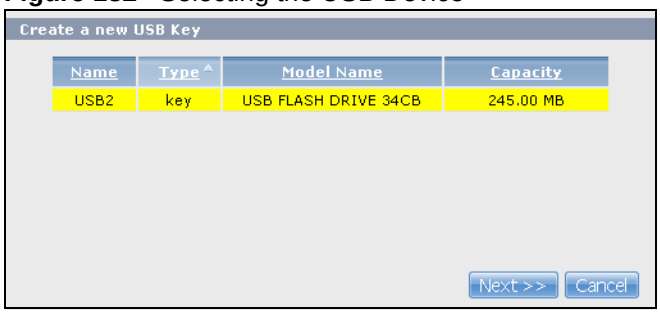
6.6.2 USB Key Creation

When you create a volume encrypted by a USB key, click the **Create USB Drive** button to open a series of screens for creating a volume encryption password and storing it on a connected USB device.

6.6.2.1 Selecting the USB Device

When you click the **Create USB Drive** button a screen displays. Select the USB device on which to create the USB key and click **Next**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 132 Selecting the USB Device



The following table describes this screen.

Table 31 Selecting the USB Device

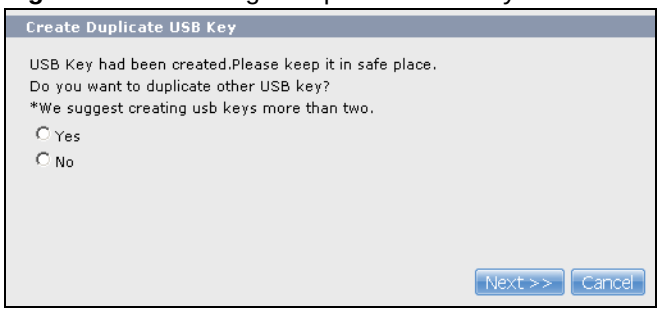
LABEL	DESCRIPTION
Name	This field shows **USB1**, **USB2**, and so on for disks connected to the NSA's USB ports.
Type	This shows whether or not the device has an encrypted volume.
Model Name	This is the device's model name that uniquely identifies it in the NSA.
Capacity	This field shows the device's storage size.
Next	Click this button to proceed.
Cancel	Click this button to discard your changes and close this screen.

6.6.2.2 Creating a Duplicate USB Key (Strongly Recommended)

Use these screens to create extra copies of your USB key in case one is lost, damaged, or stolen. Without a USB key, you cannot access the volume if it becomes locked. All of the volume's data will be unusable.

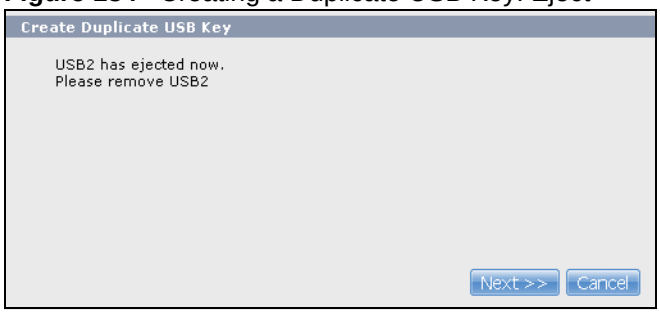
1 Select **Yes** to copy the USB key to another USB device. After the duplicate USB key creation completes, you return to this screen so you can make another. Click **No** when you are done making USB key copies.

Figure 133 Creating a Duplicate USB Key


Create Duplicate USB Key
USB Key had been created.Please keep it in safe place.
Do you want to duplicate other USB key?
*We suggest creating usb keys more than two.
Yes
No
Next >>
Cancel

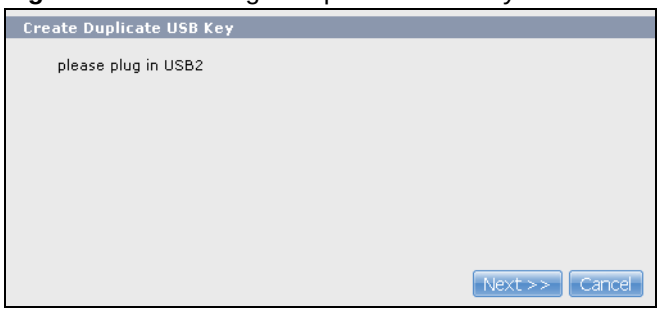
2 The NSA ejects (stops) the USB device. Remove the USB key and click **Next**.

Figure 134 Creating a Duplicate USB Key: Eject



3 Insert a different USB key and click **Next**.

Figure 135 Creating a Duplicate USB Key: Insert

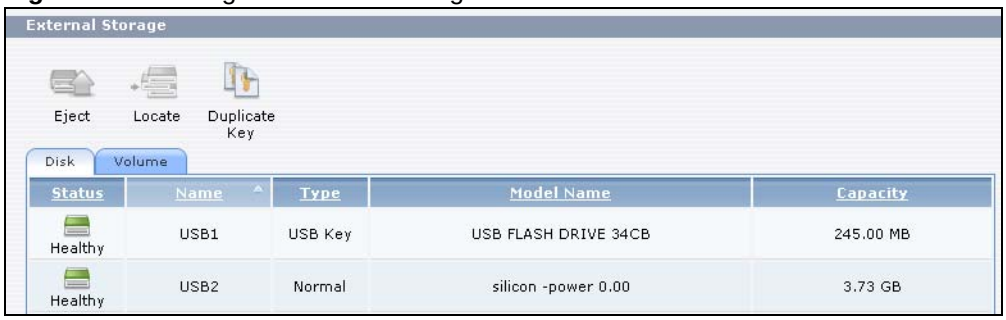


After the duplicate USB key creation completes, you return to the first USB key duplication screen (see Figure 133 on page 144) so you can make another.

6.7 External Storage Disk Screen

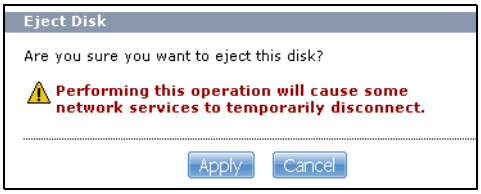
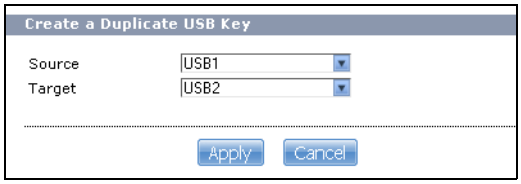
Use the external storage screens to manage the NSA's externally (USB) connected storage. Connect USB devices to the NSA's USB ports. Click **Storage** > **External Storage** to open the following screen. This screen provides information on disks connected to the NSA.

Figure 136 Storage > External Storage > Disk



The following table describes the icons in this screen.

Table 32 Storage > External Storage > Disk Icons

ICON	DESCRIPTION
	Eject Select a USB-connected device and click this icon to be able to remove the device. 
	Locate Select a USB-connected device and click this icon to have the device's LED flash so you can identify it.
	Duplicate Key Connect a USB key device and another USB device to the NSA and click this to create a copy of the key. Select the USB key device as the **Source USB**. Connect another USB device and select it as the **Destination USB**. 
	Sort Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.
	Status This icon shows if the device is functioning normally.

The following table describes the labels in this screen.

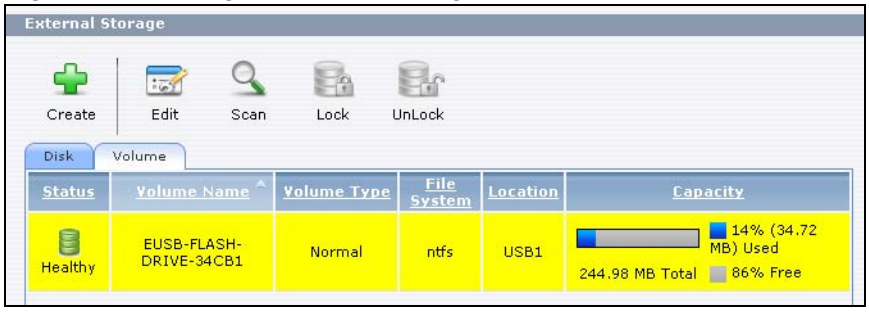
Table 33 Storage > External Storage > Disk

LABEL	DESCRIPTION
Name	This field displays the name of the NSA's USB port (**USB1** or **USB2**) to which the disk is connected. The NSA's upper USB port is **USB1** and its lower USB port is **USB2**.
Type	This shows whether or not the device has an encrypted volume.
Model Name	This is the device's model name that uniquely identifies it in the NSA.
Capacity	This field shows the device's storage size.

6.8 External Volume Screen

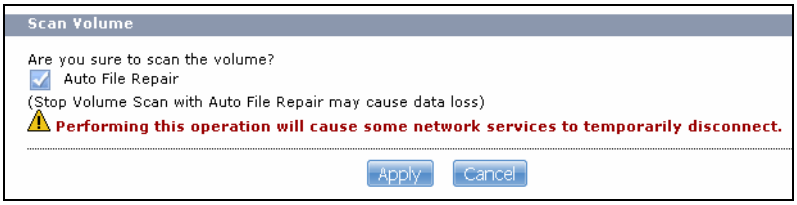
Click **Storage** > **External Storage** > **Volume** to display the external (USB-connected) volume summary screen as shown next. Use this screen to manage the NSA's external storage volumes. The NSA automatically creates volumes when you connect an external disk. You can also create other volumes.

Figure 137 Storage > External Storage > Volume



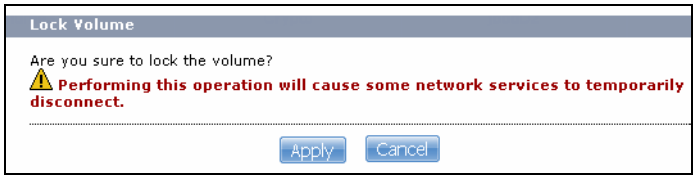
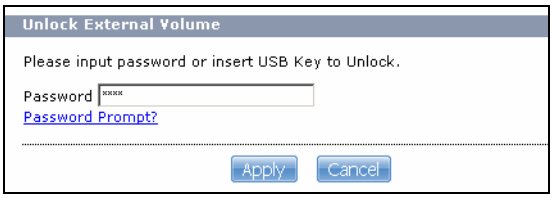
The following table describes the icons in this screen.

Table 34 Storage > External Storage > Volume Icons

ICON	DESCRIPTION
	Create Click this icon to open a screen where you can create a new storage volume.
	Edit Select a volume and click this icon to modify it's settings.
	Scan Select a volume and click this icon to check the volume's file consistency.  Note: If you have the NSA automatically attempt to repair any damaged files it finds during the scan, be careful not to cancel the scan.

Scan Volume
Are you sure to scan the volume?
Auto File Repair
(Stop Volume Scan with Auto File Repair may cause data loss)
Performing this operation will cause some network services to temporarily disconnect.
Apply
Cancel

Table 34 Storage > External Storage > Volume Icons (continued)

ICON	DESCRIPTION
	Lock If an encrypted volume is unlocked, you can select it and click this icon to lock it. No one will be able to use the volume until an administrator unlocks it. Note that if the volume was encrypted using a USB key and the USB key is connected when the NSA restarts, the NSA automatically unlocks the volume. 
	Unlock The NSA automatically locks an encrypted volume if the NSA loses power or the disk is removed. Select a locked volume and click this icon to open a screen where you can enter the volume's password or use the USB key to allow users to use the volume again.  If the USB device containing the volume's key is already inserted, remove it and re-insert it.
	Sort Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.
	Status This icon shows whether the volume is **Healthy, Locked, Unlocked,** or **Down**; see Section 6.6 on page 139. If a volume is degraded, click the

The following table describes the labels in this screen.

Table 35 Storage > External Storage > Volume

LABEL	DESCRIPTION
Volume Name	This field shows the name of the volume.
Volume Type	This field shows the volume is unencrypted (**Normal**) or encrypted (**Crypto**).
File System	This field displays the type of file system that an external (USB) volume is using.
Location	This field shows to which USB port the device is connected.
Capacity	This field shows the total size of the volume, how much is currently in use, and how much is still available.

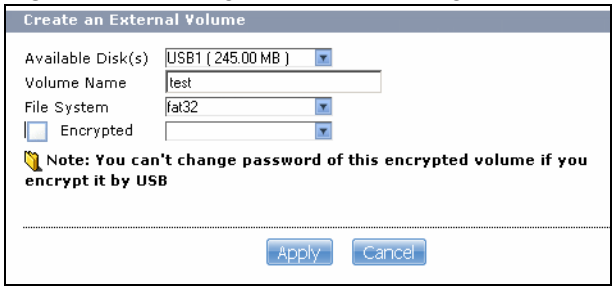
6.8.1 Creating or Editing an External Volume

Creating a volume on a USB device formats it. All data on the USB device is lost.

Click **Storage** > **External Storage** > **Volume** > **Create** to display the external (USB-connected) volume creation screen as shown next. You can also select an existing external volume and click the **Edit** icon. Use this screen to add or edit external storage volumes.

Keep an encrypted volume's password or USB key in a safe place. You cannot access a locked volume without the password or USB key. All of the volume's data will be unusable. If you use a USB key, keep backup copies. Do not use the USB key for anything else (do not store data on it or format it).

Figure 138 Storage > External Storage > Volume > Create



The following table describes this screen.

Table 36 Storage > External Storage > Volume Create

LABEL	DESCRIPTION
Available Disk(s)	Select the external (USB) device upon which you want to create the volume.
Volume Name	Type a volume name from 1 to 31 characters. To ease management, it is highly recommended that each volume use a unique name. Acceptable characters are all alphanumeric characters and " " [spaces], "_" [underscores], and "." [periods]. The first character must be alphanumeric (A-Z 0-9). The last character cannot be a space " ".

Table 36 Storage > External Storage > Volume Create (continued)

LABEL	DESCRIPTION
File System	Select the file system you want the new volume to use. If you plan to also use the USB device with another computer, it is recommended that you select the file system that the other computer uses. Windows file systems **fat32**: Newer, and more efficient than FAT16. Supports a volume size of up to 2 TB (Tera Bytes) and individual file sizes of up to 4 GB. **fat16**: Compatible with older Windows operating systems. Supports volume and file sizes of up to 2 GB. **ntfs**: The newest Windows file system. Linux file systems **ext2**: Older file system. **ext3**: The same as EXT2, but adds a journaled file system and is more robust. **reiserfs**: Offers better performance for small files. **xfs**: Offers good performance for larger files. You can also have the NSA encrypt a volume that uses the xfs file system.
Encrypted	Select this check box and an option from the drop-down list box to encrypt the volume. This option is only available when you create a volume using the xfs file system. The NSA automatically locks an encrypted volume if the NSA restarts or loses power or the disk is removed. An administrator can also manually lock the volume. Once a volume is locked, no one can use it again until an administrator unlocks it. **password**: Select this option to manually enter a password for unlocking this volume. You can also enter a password prompt. You will need to manually re-enter the key every time the NSA restarts. **USB key**: Select this option to have the NSA create a password for unlocking the volume and store the password on (another) connected USB device. Note that if the volume is later locked, the NSA automatically unlocks it if the USB device containing the key is inserted when the NSA restarts. At start up, if a USB key is inserted, the NSA automatically unlocks any volumes encrypted by it.
Password	The password fields display if you choose to encrypt the volume by manually entering a password. Enter a password for encrypting the volume.
Password (Confirm)	Re-type the password to make sure you entered it correctly.
Password Prompt	Enter a hint to help you recall the password if you forget it.
USB Key	The USB field and button display if you choose to encrypt the volume by USB key. Select a USB key device that you created previously or select a USB device that you want to make into a USB key. If the USB device is not already connected, connect it and click the **Refresh** icon. The NSA's upper USB port is **USB1** and its lower USB port is **USB2**. It is recommended that you use a USB device to store a volume key only and not also use it for storage.

Table 36 Storage > External Storage > Volume Create (continued)

LABEL	DESCRIPTION
Create USB Drive	Click this button to go to screens you can use to create a password for unlocking the volume and store the password on a connected USB device. You also use the screens to create copies of the USB key. See Section 6.6.2 on page 143 for details. Note: Create duplicate USB keys now since you cannot make them later. Without a USB key, you cannot access the volume if it becomes locked. All of the volume's data will be unusable.
Apply	Click this button to save your changes back to the NSA.
Cancel	Click this button to discard your changes and close this screen.

6.9 Technical Reference

This section contains background on JBOD and the RAID levels used on the NSAand lists some common S.M.A.R.T. attributes.

6.9.1 Storage Terminology

These are some terms that you need to know in order to understand storage systems.

- Mirroring

  In a RAID system using mirroring, all data in the system is written simultaneously to two hard disks instead of one. This provides 100% data redundancy as if one disk fails the other has the duplicated data. Mirroring setups always require an even number of drives.
- Duplexing

  Like in mirroring, all data is duplicated onto two distinct physical hard drives but in addition it also duplicates the hardware that controls the two hard drives (one of the drives would be connected to one adapter and the other to a second adapter).
- Striping

  Striping is the breaking up of data and storing different data pieces on each of the drives in an array. This allows faster reading and writing as it can be done simultaneously across disks. Striping can be done at the byte level, or in blocks. Byte-level striping means that the first byte of the file is sent to the first drive, then the second to the second drive, and so on. Block-level striping means that each file is split into blocks of a certain size and those are distributed to the various drives. The size of the blocks used is also called the stripe size (or block size).
- Parity

  In mirroring 50% of the drives in the array are reserved for duplicate data. Parity is another way to allow data recovery in the event of disk failure using calculations rather than duplicating the data. If you have 'n' pieces of data, parity computes an extra piece of data. The'n+1' pieces of data are stored on 'n+1'drives. If you lose any one of the 'n+1' pieces of data, you can recreate it from the 'n' that remain, regardless of which piece is

lost. Parity protection is used with striping, and the “n” pieces of data are typically the blocks or bytes distributed across the drives in the array. The parity information can either be stored on a separate, dedicated drive, or be mixed with the data across all the drives in the array.

In the following figures, A1, A2, A3 and so on are blocks of data from the A file. Similarly, B1, B2, B3 and C1, C2, C3 ar blocks of data from the B and C files.

6.9.2 JBOD

- Minimum number of disks: 1
- Total capacity: Sum of the member disks
- Advantages: Maximum storage capacity, especially for disks of mixed sizes. Flexibility (you can add disks to the JBOD
- Disadvantages: Not as fast or reliable as RAID.

JBOD allows you to combine multiple physical disk drives into a single virtual one, so they appear as a single large disk. JBOD can be used to turn several different-sized drives into one big drive. For example, JBOD could convert 100 GB, 200 GB, 250 GB, and 500 GB drives into one large logical drive of 1050 GB. Since data isn’t striped across disks, if one disk fails, you should just lose the data on that disk (but you may lose data in the whole array depending on the nature of the disk failure). You can add disks to the JBOD array later (using the Add disk to JBOD feature) and even remove them so JBOD offers a lot of flexibility. However JBOD read performance is not as good as RAID as only one disk can be read at a time and they must be read sequentially. The following figure shows three disks in a single JBOD array. Data is not written across disks but written sequentially to each disk until it’s full.

Table 37 JBOD

A1	**B1**	**C1**
A2	**B2**	**C2**
A3	**B3**	**C3**
A4	**B4**	**C4**
DISK 1	**DISK 2**	**DISK 3**

6.9.3 RAID 0

RAID 0 spreads data evenly across two or more disks (data striping) with no mirroring nor parity for data redundancy, so if one disk fails the entire array will be lost. The major benefit of RAID 0 is performance. The following figure shows two disks in a single RAID 0 array. Data can be written and read across disks simultaneously for faster performance.

Table 38 RAID 0

A1	A2
A3	A4
A5	A6
A7	A8
DISK 1	DISK 2

RAID 0 capacity is the size of the smallest disk multiplied by the number of disks you have configured at RAID 0 on the NSA. For example, if you have four disks of sizes 100 GB, 150 GB, 150 GB and 200 GB respectively in one RAID 0 array, then the maximum capacity is 400 GB (4 * 100 GB, the smallest disk size) and the remaining space (300 GB) is unused.

Typical applications for RAID 0 are non-critical data (or data that changes infrequently and is backed up regularly) requiring high write speed such as audio, video, graphics, games and so on.

6.9.4 RAID 1

RAID 1 creates an exact copy (or mirror) of a set of data on another disk. This is useful when data backup is more important than data capacity. The following figure shows two disks in a single RAID 1 array with mirrored data. Data is duplicated across two disks, so if one disk fails, there is still a copy of the data.

Table 39 RAID 1

A1	A1
A2	A2
A3	A3
A4	A4
DISK 1	DISK 2

As RAID 1 uses mirroring and duplexing, a RAID 1 array needs an even number of disks (two or four for the NSA).

RAID 1 capacity is limited to the size of the smallest disk in the RAID array. For example, if you have two disks of sizes 150 GB and 200 GB respectively in one RAID 1 array, then the maximum capacity is 150 GB and the remaining space (50 GB) is unused.

Typical applications for RAID 1 are those requiring high fault tolerance without need of large amounts of storage capacity or top performance, for example, accounting and financial data, small database systems, and enterprise servers.

6.9.5 RAID 10

RAID 10 (RAID 1+0) is a nested RAID where two RAID 1 arrays are stored on the physical disks with a RAID 0 array on top. It is a stripe of mirrors. RAID 1 provides redundancy while RAID 0 boosts performance. The following figure shows two disks in two RAID 1 arrays. Data is duplicated across two disks, so if one disk fails, there is still a a copy of the data. These two arrays are configured as a single RAID 0 array for faster performance.

Table 40 RAID 10

RAID 0			
RAID 1		RAID 1	
A1	A1	A2	A2
A3	A3	A4	A4
A5	A5	A6	A6
A7	A7	A8	A8
DISK 1	DISK 2	DISK 3	DISK 4

Typical applications for RAID 10 are those requiring both high performance and reliability such as enterprise servers and high-end moderate-sized database systems. RAID 10 is often used in place of RAID 1 or RAID 5 by those requiring higher performance. It may be used instead of RAID 1 for applications requiring more capacity.

6.9.6 RAID 5

RAID 5 provides the best balance of capacity and performance while providing data redundancy. It provides redundancy by striping data across three disks and keeps the parity information (AP) on the fourth disk (in each stripe). In case of disk failure, data can be recovered from the surviving disks using the parity information. When you replace the failed disk, the reconstructed data is written onto the new disk. Re-synchronize the array to have it return to its original state. The following example shows data stripped across three disks (A1 to A3 in the first strip for example) with parity information (AP) on the fourth disk.

Table 41 RAID 5

A1	**A2**	**A3**	**AP**
B1	**B2**	**BP**	**B3**
C1	**CP**	**C2**	**C3**
DP	**D1**	**D2**	**D3**
DISK 1	**DISK 2**	**DISK 3**	**DISK 4**

The capacity of a RAID 5 array is the smallest disk in the RAID set multiplied by one less than the number of disks in the RAID set. For example, if you have four disks of sizes 150 GB, 150 GB, 200 GB and 250 GB respectively in one RAID 5 array, then the maximum capacity is 450 GB (3 * 150 GB, the smallest disk size) and the remaining space (300 GB) is unused.

Typical applications for RAID 10 are transaction processing, relational database applications, enterprise resource planning and other business systems. For write-intensive applications, RAID 1 or RAID 1+0 are probably better choices, as the performance of RAID 5 will begin to substantially decrease in a write-heavy environment.

6.9.7 Hot-spare

A RAID 1 or RAID 5 array with a hot-spare operates as a three-disk RAID 1 or RAID 5 array with the fourth disk on standby. The standby disk automatically comes into play if a disk in the array fails. The advantage of a hot-spare is that if a disk fails, then the array resynchronizes automatically with the standby disk and operates at healthy array speed after the resynchronization.

You need four hard disks installed to use RAID 10, RAID 5 or RAID 5 with hot-spare.

6.9.8 RAID and Data Protection

If a hard disk fails and you're using a RAID 1, RAID 10, or RAID 5 array then your data will still be available (but at degraded speeds until you replace the hard disk that failed and re-synchronize the array). However, RAID cannot protect against file corruption, virus attacks, files incorrectly deleted or modified, or the NSA malfunctioning. See Section 9.1 on page 197 for what you should use in these cases to protect data on your NSA.

6.9.9 S.M.A.R.T Attributes

The following table describes some common S.M.A.R.T. attributes. If a higher or lower raw attribute value is better, it is indicated in the **BETTER** column. Since S.M.A.R.T. attributes and their definitions vary by manufacturer, refer to the hard drive manufacturer for details about the attributes your hard drive supports.

Table 42 S.M.A.R.T. Attributes

ID	ATTRIBUTE NAME	BETTER	DESCRIPTION
01	Read Error Rate	Low	Shows the rate of hardware read errors. If this is not zero, there is a problem with the disk surface or the read/write heads.
02	Throughput Performance	High	This is the hard drive's general (overall) throughput performance. A decreasing value indicates a problem.
03	Spin-Up Time	Low	This is the average number of milliseconds the hard drive took for spindle spin up (from zero RPM to fully operational).
04	Start/Stop Count		The total number of spindle start and stop cycles.
05	Reallocated Sectors Count	Low	Total number of reallocated sectors on the hard drive. When the hard drive detects a read/write/verification error, it marks the sector as "reallocated" and transfers the data to a specially reserved (spare) area. The process is also known as remapping with "reallocated" sectors known as remaps. The more sectors the hard drive has to reallocate, the slower read and write speeds become.
06	Read Channel Margin		This is the margin of a channel when it reads data.
07	Seek Error Rate	Low	This is the rate of the magnetic heads' seek errors. A failure in the mechanical positioning system, such as servo damage or a thermal widening of the disk, results in seek errors. An increasing number of seek errors indicate the condition of the disk surface and the mechanical subsystem are worsening.
08	Seek Time Performance	High	This is an average performance indicator for the seek operations of the magnetic heads. Mechanical subsystem problems cause this value to decrease.
09	Power-On Hours (POH)	Low	This is how many hours the hard drive has been in a power-on state. The raw value lists the total number of hours (or minutes, or seconds depending on the manufacturer).
10	Spin Retry Count	Low	This is the total number of spin start retry attempts. This is the number of attempts to spin up to fully operational speed the hard drive has made when the first attempt did not succeed. An increase in this value is an indicator of hard disk mechanical subsystem problems.
11	Recalibration Retries	High	This is the number of times recalibration was requested when the first attempt did not succeed. A decrease in this value is an indicator of hard disk mechanical subsystem problems.

Table 42 S.M.A.R.T. Attributes (continued)

ID	ATTRIBUTE NAME	BETTER	DESCRIPTION
12	Device Power Cycle Count		This is the number of times the hard drive has gone through a full power on and power off.
13	Soft Read Error Rate	Low	This is the number of uncorrected read errors the hard drive has reported. If this is not zero, back up your data.
190	Airflow Temperature	Low	This indicates the temperature of the airflow measured by a Western Digital hard drive.
190	Temperature Difference from 100	High	This indicates the value of 100 - the temperature in degrees Celsius. Manufacturers can set a minimum threshold that corresponds to a maximum temperature.
191	G-sense error rate	Low	This is the number of mistakes caused by impact loads.
192	Power-off Retract Count	Low	This is how many times the heads are loaded off the media.
193	Load/Unload Cycle	Low	This is the number of load and unload cycles into head landing zone position.
194	Temperature	Low	This is the hard drive's internal temperature.
195	Hardware ECC Recovered	High	This is the time between ECC (Error Correction Code)-corrected errors.
196	Reallocation Event Count	Low	This is the total number of reallocation (remap) operations. The raw value is the total attempts to move data from reallocated sectors to a spare area. Successful and unsuccessful attempts are both included.
197	Current Pending Sector Count	Low	This is the number of unstable sectors awaiting reallocation. If the sector is later successfully written or read, this value decreases and reallocation is not performed. Only failed write attempts cause a reallocation, not read errors. This can be difficult to test since only direct I/O writes to the disk cause reallocations, not cached writes.
198	Uncorrectable Sector Count	Low	This is the number of errors reading or writing a sector that were not correctable. An increase in this value is an indicator of disk surface defects or mechanical subsystem problems.
199	UltraDMA CRC Error Count	Low	This is the number of data transfer errors through the interface cable according to the ICRC (Interface Cyclic Redundancy Check).
200	Write Error Rate / Multi-Zone Error Rate	Low	This is the total number of errors in writing sectors.
201	Soft Read Error Rate	Low	This is the number of read/write head off-track errors. If the value is not zero, make a backup.
202	Data Address Mark Errors	Low	This is the number of data address mark errors. This could also be a different, manufacturer-specific attribute.
203	Run Out Cancel	Low	This is the number of ECC (Error Correction Code) errors.
204	Soft ECC Correction	Low	This is the number of errors corrected by software ECC (Error Correction Code).
205	Thermal Asperity Rate (TAR)	Low	This is the number of thermal asperity errors. Thermal asperity is a read signal spike caused by sensor temperature rise due to touching the disk surface or contaminant particles.
206	Flying Height		This is the height of the hard drive's read/write heads above the disk surface.

Table 42 S.M.A.R.T. Attributes (continued)

ID	ATTRIBUTE NAME	BETTER	DESCRIPTION
207	Spin High Current		This is the quantity of high current used to spin up the drive.
208	Spin Buzz		This is the number of buzz routines to spin up the drive. When the arm holding the read/write heads is stuck, the motor driving it tries to oscillate the arm to free it. This causes an audible vibration.
209	Offline Seek Performance		This is the hard drive's seek performance during offline operations. Offline operations are tests the drive does itself as opposed to those that an external diagnostic tool has it do. Seek performance is how quickly the drive moves from track to track.
220	Disk Shift	Low	This is how far the disk has moved relative to the spindle (this kind of shift is usually due to shock).
221	G-Sense Error Rate	Low	This is the number of errors that have resulted from external vibration and shock.
222	Loaded Hours		This is how long the hard drive has operated under data load (this requires movement of the magnetic head armature).
223	Load/Unload Retry Count		This is how many time the magnetic head has changed position.
224	Load Friction	Low	This is resistance caused by friction in mechanical parts during operation.
225	Load/Unload Cycle Count	Low	This is the total number of load cycles.
226	Load 'In'-time		This is the total time that the magnetic heads actuator has had a load (not been in the parking area).
227	Torque Amplification Count	Low	This is the number of attempts to compensate for variations in platter speed.
228	Power-Off Retract Cycle	Low	This is how many times the magnetic armature was automatically retracted because the power was cut.
230	GMR Head Amplitude		This is the amplitude of thrashing (or the distance of repetitive forward and reverse head motion).
231	Temperature	Low	This is the hard drive's temperature.
240	Head Flying Hours		This is the total time that the head has been positioning.
250	Read Error Retry Rate	Low	This is the number of errors in reading from the disk.

7

Network Screens

This chapter discusses the network screens.

7.1 Network Screens Overview

Use the network screens to configure the NSA's network settings so computers can access it.

7.1.1 What You Can Do in the Network Screens

- Use the **TCP/IP** screen (Section 7.2 on page 160) to configure the NSA's TCP/IP network connection settings such as the teaming mode and IP addresses.
- Use the **Windows/CIFS** screens (Section 7.3 on page 164) to configure CIFS settings such as your Windows/CIFS server name and workgroup name so programs like Windows Explorer can access the NSA.
- Use the **NFS** screens (Section 7.4 on page 168) to configure NFS settings so computers using the NFS file system can access the NSA.

7.1.2 What You Need to Know About the Network Screens

Teaming Mode

The teaming mode sets how the NSA's two Gigabit Ethernet interfaces behave. They can act independently, one can back up the other, they can share the traffic load, or they can be trunked into a logical link.

IP Address

The NSA needs an IP address(es) to communicate with the computers on your network. The NSA can get an IP address automatically if you have a device on your network that gives them out. Or you can assign the NSA a static (fixed) IP address.

DNS Server Address

A DNS (Domain Name System) server maps domain names (like www.zyxel.com) to their corresponding IP addresses. This lets you use domain names to access web sites without having to know their IP addresses. The NSA can receive the IP address of a DNS server automatically (along with the NSA's own IP address). You can also manually enter a DNS server IP address in the NSA.

DHCP

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the NSA as a DHCP client which means it is set to receive an IP address from a DHCP server. The NDU can help you discover the IP address of the NSA.

Alternatively, configure a static IP address for the NSA.

Jumbo Frames

Jumbo frames are Ethernet frames larger than 1500 bytes. They enable data transfer with less overhead. The bigger the frame, the better the network performance.

Windows/CIFS

Common Internet File System (CIFS) is a standard protocol supported by most operating systems in order to share files across the network.

CIFS runs over TCP/IP but uses the SMB (Server Message Block) protocol found in Microsoft Windows for file and printer access; therefore, CIFS will allow all applications, not just Web browsers, to open and share files across the Internet.

NFS

NFS (Network File System) is a protocol most commonly used on Unix-like systems in order to share files across the network.

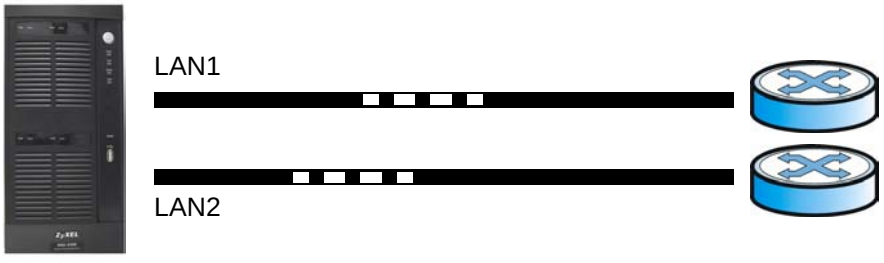
7.2 TCP/IP Screen

Teaming Mode

Here are the teaming mode settings the NSA's two Gigabit Ethernet interfaces can use.

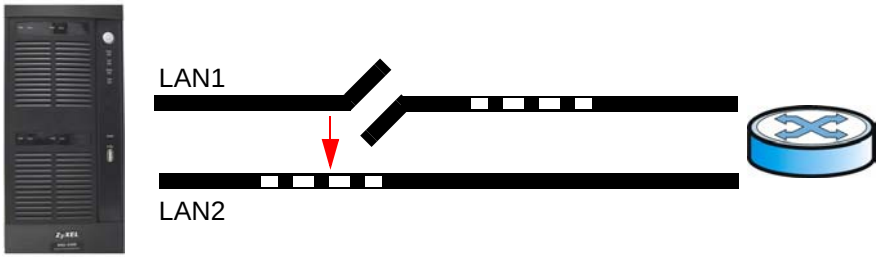
Stand Alone: LAN1 and LAN2 each use a unique IP address. These IP addresses are independent of each other.

Figure 139 Stand Alone Teaming Mode



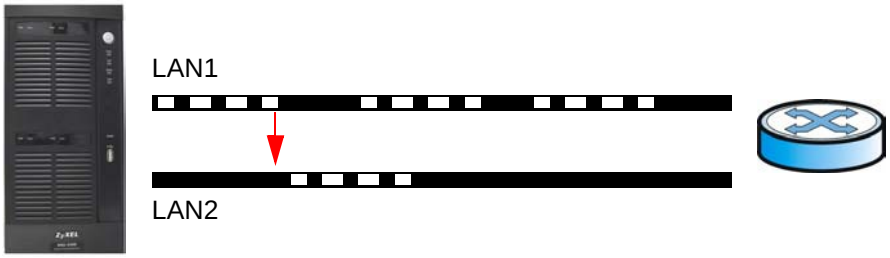
Fault Tolerance: LAN2 serves as a backup (fail-over) for the LAN1. Both Gigabit Ethernet interfaces are connected to the same subnet. There is one IP address. If LAN1 loses its connection, LAN2 takes over LAN1's IP address and traffic.

Figure 140 Fault Tolerance Teaming Mode



Load Balancing: This distributes the traffic load across LAN1 and LAN2. LAN1 and LAN2 are on the same subnet with the same IP address. It also includes backup functionality (fault tolerance).

Figure 141 Load Balancing Teaming Mode



Link Aggregation: This uses IEEE 802.3ad port link aggregation to combine LAN1 and LAN2 into a single logical link with greater bandwidth. Both interfaces use the same IP address and MAC address. It also includes fault tolerance and load balancing. Connect LAN1 and LAN2 to the same Ethernet switch. The switch must also have IEEE 802.3ad port link aggregation (also called trunking) enabled for the two interfaces connected to the NSA.

Figure 142 Link Aggregation Teaming Mode

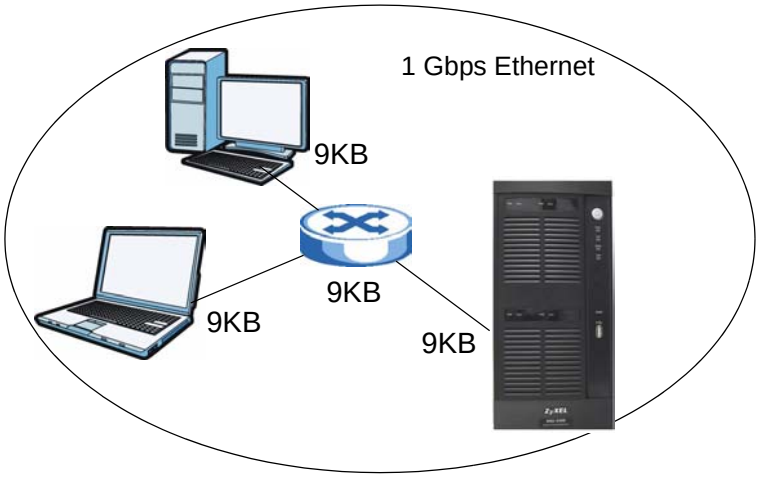
Jumbo Frames

To use jumbo frames, your network must support 1 Gbps transmissions (Gigabit Ethernet). All of your network devices (computer Ethernet cards and switches, hubs, or routers) must also support the same size of jumbo frames that you specify in the NSA.

If you enable jumbo frames on the NSA in a network that does not support them, you will lose access to the NSA. If this occurs, you will have to restore the factory default configuration. Use the **RESET** button or the Web Configurator.

In the following example, the NSA has jumbo frames enabled and set to 9KB frames. This means the computer, notebook computer, and switch must also have jumbo frames enabled and be capable of supporting 9KB frames.

Figure 143 Jumbo Frames



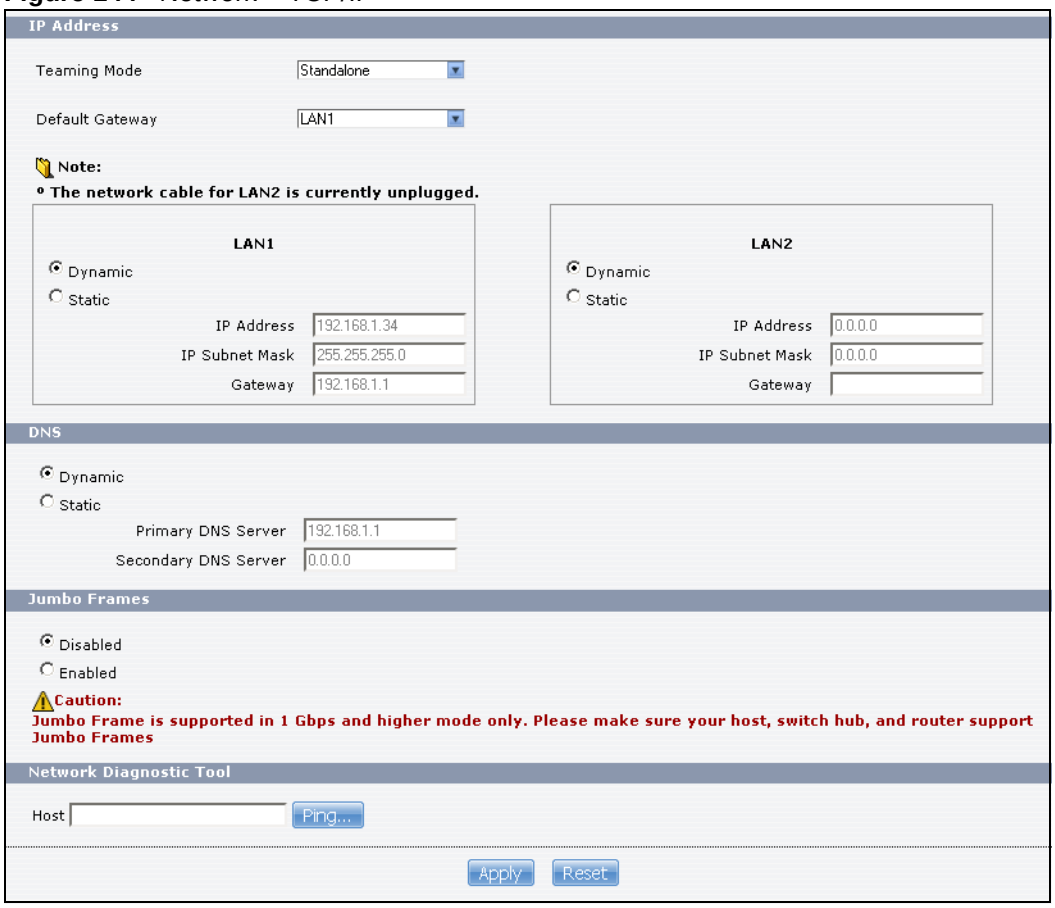
7.2.1 Configuring the TCP/IP Screen

Use the **Network > TCP/IP** screen to assign the NSA a dynamic or static IP address(es), subnet mask, default gateway and DNS servers.

The NSA automatically restarts its network services after you apply changes in the **TCP/IP** or **Windows/CIFS** screens.

Click **Network** > **TCP/IP** to access the **Network > TCP/IP** screen.

Figure 144 Network > TCP/IP



The following table describes the labels in this screen.

Table 43 Network > TCP/IP

LABEL	DESCRIPTION
Teaming Mode	Select how to use the NSA's two Gigabit Ethernet interfaces. **Stand Alone**: Select this option to use a separate IP address on each of the two Gigabit Ethernet interfaces. **Fault Tolerance**: Select this option to use the LAN2 Gigabit Ethernet interface as a fail-over (backup) for the LAN1 Gigabit Ethernet interface. Both Gigabit Ethernet interfaces are connected to the same subnet. There is one IP address. If LAN1 loses its connection, LAN2 takes over the IP address and traffic. **Load Balancing**: Select this option to use both Gigabit Ethernet interfaces on the same subnet with the same IP address. The NSA distributes the traffic load across both interfaces. **Link Aggregation**: Select this option to use IEEE 802.3ad port link aggregation to combine the two Gigabit Ethernet interfaces into a single logical link. Connect both Gigabit Ethernet interfaces to the same device. The peer device must also have IEEE 802.3ad port link aggregation enabled for the two interfaces connected to the NSA. Both interfaces use the same IP address. If one interface loses its connection, the NSA continues to use the other interface.
LAN	Use this section to configure the NSA's IP address or IP addresses (configure LAN1 and LAN2 separately when the **Teaming Mode** is set to **Stand Alone**).
Dynamic	Select the **Dynamic** checkbox to have a DHCP server automatically assign an IP address to your NSA. If none is assigned, then the NSA reverts to the default IP address of 192.168.1.3.

Table 43 Network > TCP/IP

LABEL	DESCRIPTION
Static	Select the **Static** checkbox for the NSA to use fixed TCP/IP information. You must fill in all of the following fields.
IP Address	Type an IP address in this field.
IP Subnet Mask	Type an IP subnet mask in this field.
Gateway	Type a default gateway address in this field.
DNS	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. If you have the IP address(es) of the DNS server(s), enter them.
Dynamic	Select the checkbox to have the DHCP server automatically assign a DNS server address to your NSA.
Static	Select the checkbox to choose a static DNS server address. Type the DNS server IP address(es) into the fields below.
Primary DNS Server	Type a primary DNS server IP address.
Secondary DNS Server	Type a secondary DNS server IP address.
Jumbo Frames	Jumbo frames improve network performance. You must have a 1 Gbps (Gigabit Ethernet) network that supports jumbo frames. Select the largest size of frame that all of your network devices (including computer Ethernet cards and switches, hubs, or routers) support. Note: If you enable jumbo frames on the NSA in a network that does not support them, you will lose access to the NSA. If this occurs, you will have to restore the factory default configuration.
Network Diagnostic Tool	Use this section to test the network connection to a particular IP address or domain name. Select an address or type it into the field. Then click **Ping** to have the NSA send a packet to test the network connection. If the NSA is able to “ping” the host, the network connection is OK.
Apply	Click **Apply** to save your TCP/IP configurations. After you click **Apply**, the NSA restarts. Wait until you see the **Login** screen or until the NSA fully boots and then use the NDU to rediscover it.
Reset	Click **Reset** to begin configuring this screen afresh.

7.3 Windows/CIFS

Use this screen to configure your CIFS settings. In this screen you can set your server name and specify if your NSA is a part of a workgroup or domain.

CIFS is always enabled on the NSA.

The NSA automatically restarts its network services after you apply changes in the **TCP/IP** or **Windows/CIFS** screens.

Workgroup Security Mode

A workgroup is a group of computers on a network that can share files. On the NSA, use Workgroup Security Mode if the user names and passwords for these computers are maintained on the NSA. This is suitable for users using the Common Internet File System (CIFS) protocol for remote file access in a small-to-medium sized office.

Windows Domain Security Mode

A domain is a group of computers that are part of a network and share a common directory database. On the NSA, use Windows domain security mode if you want centralized management of shared resources, services and user on a centralized Windows-based domain controller. You can create users and groups on the centralized Windows-based domain controller such as an active server directory, and the NSA checks this list when authenticating users and/or groups that seek access to a share. This is suitable for a large number of CIFS users where accounts are stored on an external server.

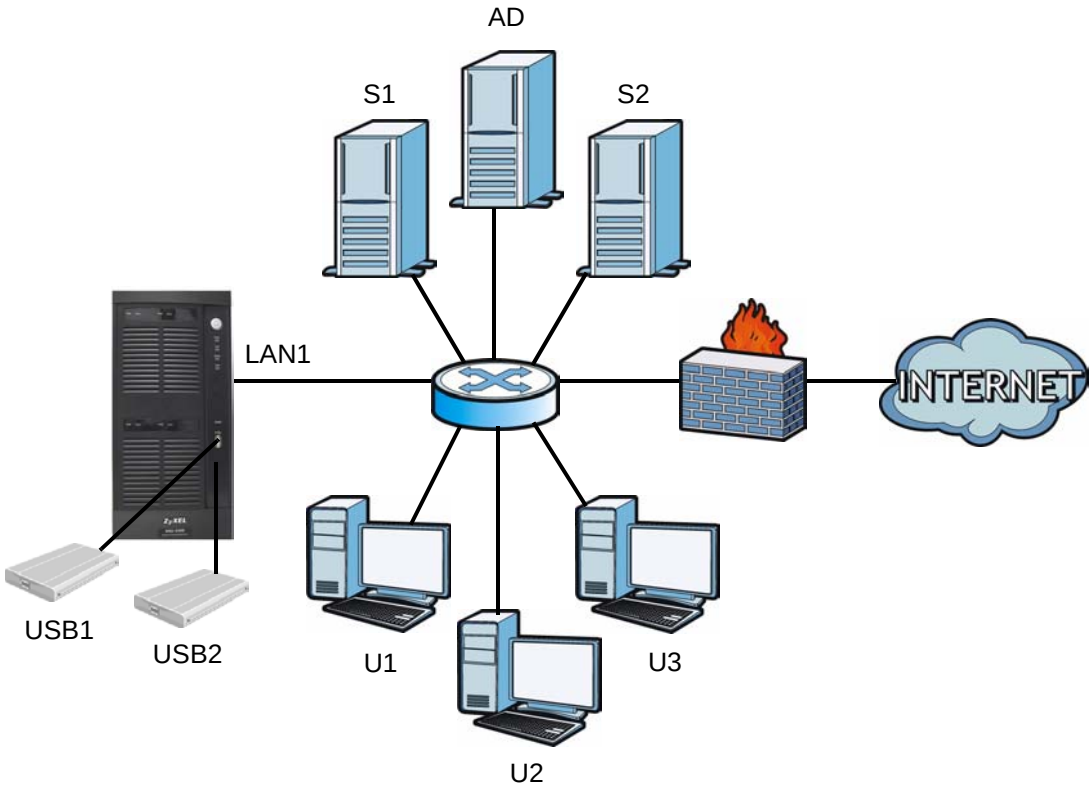
A domain is organized in levels and is administered as a unit with common rules and procedures. Each domain has a unique name. You must be logged on as an administrator to your local computer and have a valid user name and password to join your computer to a domain. If you do not know which user name and password to use, contact your network administrator.

The NSA automatically synchronizes its time and date with those on the external domain controller.

Active Directory Example

The next figure shows an example application for the NSA in a small office network. AD is an Active Directory that contains the user names and passwords of all users that are allowed access to the NSA. Users (U1, U2, U3) can all back up and share data on the NSA. Important data stored on servers S1 and S2 may be also stored there. It is recommended that you place the NSA behind a firewall and/or IDP device for protection.

Figure 145 Active Directory Example Application

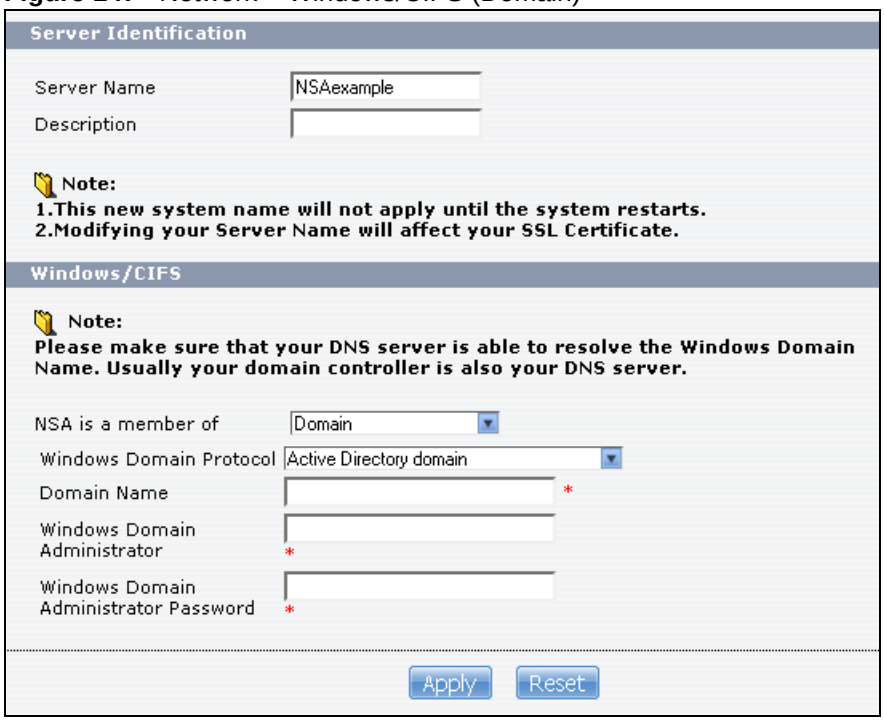


7.3.1 Windows/CIFS Screen

Click **Network** > **Windows/CIFS** to display this screen.

Figure 146 Network > Windows/CIFS (Workgroup)

Figure 147 Network > Windows/CIFS (Domain)


Server Identification
Server Name
NSAexample
Description
Note:
1.This new system name will not apply until the system restarts.
2.Modifying your Server Name will affect your SSL Certificate.
Windows/CIFS
Note:
Please make sure that your DNS server is able to resolve the Windows Domain Name. Usually your domain controller is also your DNS server.
NSA is a member of
Domain
Windows Domain Protocol
Active Directory domain
Domain Name
Windows Domain Administrator
Windows Domain Administrator Password
Apply
Reset

The following table describes the labels in these screens.

Table 44 Network > Windows/CIFS

LABEL	DESCRIPTION
Server Identification	
Server Name	Enter a name to identify your NSA on the network in this field. By default the NSA uses “NSA” and the last four digits of the NSA’s LAN 1 MAC address.
Description	Enter additional identification information for the NSA (optional).
Windows/CIFS	
NSA is a member of	A workgroup is a group of computers on a network that can share files. These user accounts are maintained on the NSA. A domain is a group of computers that are part of a network and share a common directory database. Domain users and groups are created on a centralized Windows-based domain controller. Select either **Workgroup** or **Domain** from the drop-down list box. This field becomes read-only after the NSA joins a domain.
Workgroup Name	Type your workgroup name in this field if you selected **Workgroup** from the field above. The following fields apply if you selected **Domain**.
Windows Domain Protocol	Select a windows domain protocol if you selected **Domain** above. Choose **NT4 Domain** if your server uses a Windows NT operating system and **Active Directory Domain** if it uses a Windows 2000 or later operating system.
Domain Name	Type the domain name of the Windows server domain controller. The name can be up to 255 characters long. The NSA’s DNS server must be able to resolve this domain name.
Windows Domain Administrator	Administrator is the default **Windows Domain Administrator**.

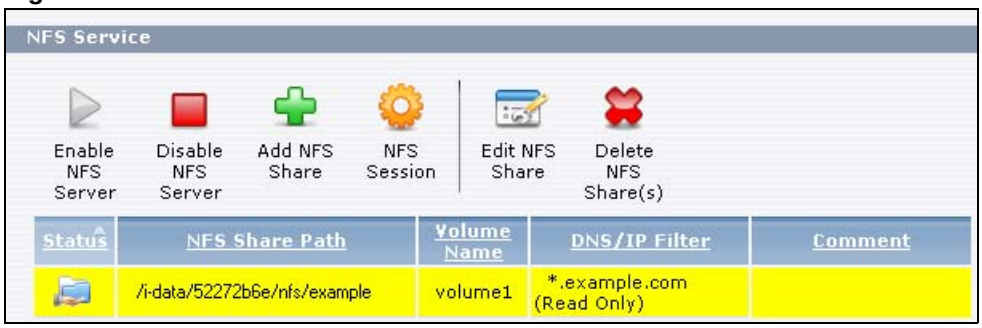
Table 44 Network > Windows/CIFS (continued)

LABEL	DESCRIPTION
Windows Domain Administrator Password	Type a password associated with the **Windows Domain Administrator**.
Test Connection	This button appears after the NSA joins a domain. Click it to check if the NSA can communicate with the Windows server domain controller.
Leave Domain	The **Leave Domain** button appears after the NSA joins a domain. Click **Leave Domain** to display options for having the NSA exit the domain. Select **Gracefully Leave Domain** to have the NSA notify the Windows server domain controller that the NSA is leaving the domain. You must also enter the Windows domain administrator password. This option is only available with active directory domains. Click **Forcefully Leave Domain** to have the NSA leave the domain without notifying the Windows server domain controller.
Apply	Click here to save your changes back to the NSA.
Reset	Click **Reset** to begin configuring this screen afresh.

7.4 NFS Screen

Click **Network** > **NFS** to display the NFS screen. Configure this screen to let computers use NFS to access the NSA.

Figure 148 Network > NFS



The following table describes the icons in this screen.

Table 45 Network > NFS Icons

ICON	DESCRIPTION
	Enable NFS Server Click this icon to allow access to the NFS shares.
	Disable NFS Server Click this icon to stop access to the NFS shares.
	Add NFS Share Click this icon to create a new NFS share.

Table 45 Network > NFS Icons (continued)

ICON	DESCRIPTION
	Edit NFS Share Select an existing NFS share and click this icon to open a screen where you can change the share's settings.
	NFS Session Click this icon to open a screen that shows who is currently connected to the NSA using NFS.
	Delete NFS Share(s) Select an existing NFS share and click this icon to remove the share.
	Sort Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.
	Status This icon shows the NFS share's current status. It can be valid (usable) or invalid (deleted).

The following table describes the labels in this screen.

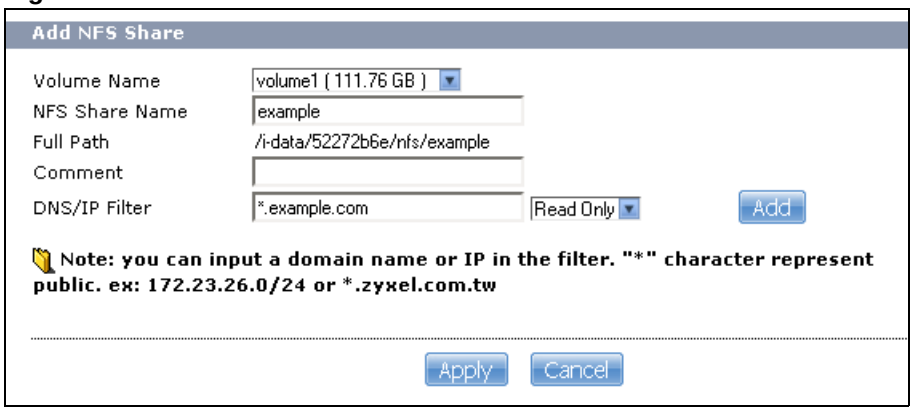
Table 46 Network > NFS

LABEL	DESCRIPTION
NFS Share Path	This field identifies the location of the NFS share in the NSA. Users need to use this share path to mount the NFS share as a drive on their computers.
Volume Name	This field identifies the volume that the share is in.
DNS/IP filters	This field displays the domain name or IP address filters configured for controlling access to the share.
Comment	This field displays any descriptive text added for the share.

7.4.1 Add or Edit NFS Share Screen

Click **Network** > **NFS** > **Add NFS Share** (or **Edit NFS Share**) to display the screen where you can configure a share for systems to use NFS to access.

Figure 149 Network > NFS > Add NFS Share



The following table describes the labels in this screen.

Table 47 Network > NFS > Add NFS Share

LABEL	DESCRIPTION
Volume Name	Select the volume upon which you want to create the NFS-enabled share.
Share Name	Enter the name of the shared folder. The text may consist of 1 to 106 characters. See Share Name Details on page 170 for details.
Full Path	This field displays the complete location of the share in the NSA.
Comment	Add descriptive text to help you identify the share.
DNS/IP Filter	To control access to the NFS share, configure filters based on domain names and IP addresses. Enter a domain name or IP address and select the appropriate level of access. You can also just use a * to indicate any. **read-only**: The users can view the files in the share but not delete them or add files. **read-write**: The users have full access to the share and can read, delete, and add files.
Add	Click this button to display another field for entering a DNS or IP filter.
remove	Click this button to remove the DNS or IP filter field.
Apply	Click to save your changes.
Cancel	Click to discard changes and close the window.

Share Name Details

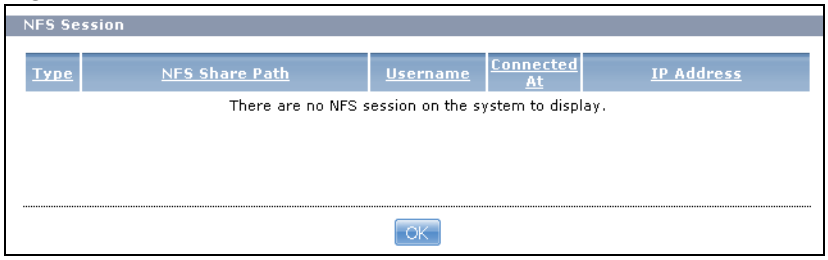
Use any character except double quotes (“), single quotes (‘), slashes (\ or /), square brackets ([ ]), colons (:), semi-colons (;), angle brackets (< >), the plus sign (+), semi-colons (;), commas (,), question marks (?), asterisks (*), the pound sign (#), tab ( ), and the equals sign (=).

- Spaces are not allowed.
- Share names must be unique (they cannot be the same as other share names).
- Share names cannot use names reserved for “automatic shares” of external USB disk volumes be unique, for example, “USB[0-9]{1,2}”, that is, a share named “USB” followed by a one or two digit number).

7.4.2 NFS Session Screen

Click **Network** > **NFS** > **NFS Session** to display the NFS session screen. This screen shows which users are currently connected to the NSA using NFS.

Figure 150 Network > NFS > NFS Session



The following table describes the labels in this screen.

Table 48 Network > NFS > NFS Session

LABEL	DESCRIPTION
Type	This shows that this is an NFS connection to the NSA.
NFS Share Path	This displays the complete location of the NFS share in the NSA.
Username	This displays the name of the user connected to the NSA.
Connected At	This displays the date and time the user last connected to the NFS share in year-day-month hour:minute:second, format.
IP Address	This displays the IP address of the computer connected to the NSA.
OK	Click **OK** to close the window.

8

Sharing Screens

8.1 Overview

Use the NSA's **Sharing** screens to manage user accounts, groups of users, and shares.

8.1.1 What You Can Do In The Sharing Screens

- Create and manage user accounts. See Section 8.2 on page 175 for details.
- Create and manage groups. See Section 8.3 on page 182 for details.
- Create and manage shares. See Section 8.4 on page 186 for details.

8.1.2 What You Need to Know About The Sharing Screens

Local User/Group

A local user or group is one created on the NSA when the NSA is in workgroup mode. (A workgroup is a collection of computers on a Windows network that can share files, printers, Internet access, and so on.)

Domain User/Group

A domain user or group is created on a centralized Windows-based domain controller. This list is used by the NSA when authenticating accounts and/or groups that seek access to a share.

If a user belongs to different groups with different access rights to the same share, then the more restrictive access right applies. That is, deny access overrides read access and read-write access. For example, let's say that user Joe belongs to the Sales group. He has read access to the MIS share. The Sales group is denied access to the MIS share, however. Therefore, Joe is also denied access to it due to the fact that he's in a more restrictive group.

More restrictive access rights override less restrictive ones.

In Conflict

A user account is "in conflict" when the account name that exists on a network-attached storage device also exists on the domain controller. See Section 8.2.0.1 on page 177 for more.

Share

A share is a set of access permissions mapped to a specific folder on a volume. It is equivalent to the Windows concept of a shared folder. You must have an internal volume before you can create shares.

Volume

A volume is a storage area on a single disk or spread across a number of disks (typically known as a disk array, or RAID) within a single file system.

XFS

XFS is journaled file system that allows for files as large as 16 terabytes. Due to the system's design, it does not easily support snapshots. Instead, it was designed with the intention that a logical volume manager would handle the snapshot/snapshot restoration process. The NSA-2401 utilizes XFS for its internal file system.

Logical Volume

A logical volume is the portion of a physical hard disk drive that allows data to be written and read. It is represented in your computer's operating system as a drive with a letter and is sub-divided into its component files and folders. For example, on a typical home computer the logical volume that exists on the hard drive that hosts the Windows operating system is most often labeled the "C" drive. A physical hard disk drive can contain a single logical volume or it can be partioned into multiple logical volumes. Furthermore, with the assistance of a logical volume manager, a logical volume can actually span multiple physical hard disk drives.

Logical Volume Manager

A logical volume manager is tool that allows system administrators greater flexibility in setting up and managing their system's storage allocation. With it, an administrator can create, delete, move and resize any number of logical volumes at will.

Snapshot

A snapshot is a "point-in-time" copy of data on a logical volume. Later, as new snapshots of the volume are made, only those bits of data that have changed from the original snapshot are duplicated. This allows a system to create instant backups on the fly without requiring a user to stop working or temporarily abandon the machine. Moreover, snapshots take up a fraction of the space of traditional full-volume backups.

Network-Attached Storage (NAS)

A NAS is basically a computer that is connected to a network and which provides additional storage capabilities to users and groups. NAS solutions most often serve as backup destinations because they come with multiple hard disk drives and numerous redundancy features in case any given drive fails.

Access Control List (ACL)

This is a list of read/write permissions associated with specific files and/or folders. Account names added to the list are linked to the files and folders that they are allowed to access, along with what kinds of actions they are allowed to perform with those files and folders.

Conflicting Share Access and ACL Settings

If the share's access permissions and the access permissions defined in the ACL differ, the NSA applies whichever is more restrictive. For example, if the share allows a user access but the ACL setting does not, the NSA does not give the user access. Also, if the ACL setting allows a user access but the share's settings do not, the NSA does not give the user access.

Finding Out More

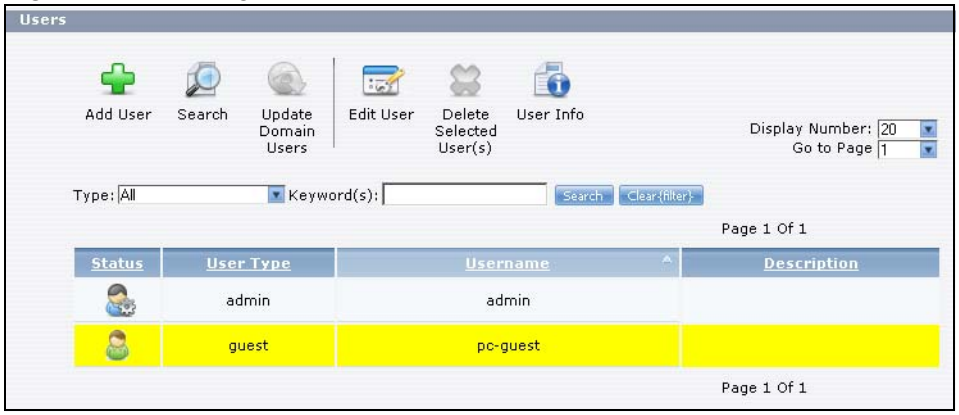
See Section 3.2 on page 55 for a tutorial on configuring the sharing screens.

See Section 3.3 on page 61 for a tutorial on using shares.

8.2 Users

Click **Sharing** > **Users** to open this screen where you can create and manage user accounts for the NSA's file services.

Figure 151 Sharing > Users



The following table describes the icons in this screen.

Table 49 Sharing > Users Icons

ICON	DESCRIPTION
	Add User Click this icon to open the **Create a New Account** screen, where you can add new user accounts. See Section 8.2.1 on page 178 for details.
	Search Click this icon to display the search filters which you can use to search for user accounts by type or keyword.
	Update Domain Users Click this icon to update the list of domain users by connecting to domain controller and retrieving the latest list of users and groups. Note: If a user is deleted on the domain controller but the NSA-2401 domain user list is not up-to-date, then the user cannot log in since authentication is handled by the domain controller.

Table 49 Sharing > Users Icons (continued)

ICON	DESCRIPTION
	Edit User Select a user account from the list, then click this icon to edit their account name, group membership, password, and volume quota. See Section 8.2.1 on page 178 for details.
	Delete Selected Users Select a user account from the list, then click this icon to remove it.
	User Info Select a user account from the list, then click this icon to view their quota and group information. See Section 8.2.2 on page 181 for details.
	Sort Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.
	Local User Indicates a local user account.
	Domain User Indicates a domain user account.
	Administrator Indicates an administrator account.
	Conflict Local User Indicates a local user account in conflict. See Section 8.2.0.1 on page 177 for more information.
	Conflict Domain User Indicates a domain user account in conflict. See Section 8.2.0.1 on page 177 for more information.

The following table describes the labels in this screen.

Table 50 Sharing > Users

LABEL	DESCRIPTION
Display Number	Set the number of user accounts displayed per page.
Go to Page	Select a page number of user accounts to display.
Type	This field displays when you click the **Search** icon. Use it to filter search results according to the user account type selected.
Keyword(s)	This field displays when you click the **Search** icon. Enter a specific word for which to search. The default is all words.
Search	This button displays when you click the **Search** icon. Click to begin searching according to the search parameters you set. If you choose not to set any search parameters, then the defaults for each filter is used.
Clear{filter}	This button displays when you click the **Search** icon. Click to reset all the search filters back to their default settings.
Previous & Next	Click **Previous** to cycle back through the pages of users, and **Next** to cycle forward through them.
Status	This icon displays the account as either a **Conflict User**, a **Local User**, a **Domain User**, or an **Admin User**.

Table 50 Sharing > Users (continued)

LABEL	DESCRIPTION
User Type	This field displays whether the account is a user or an administrator.
User Name	This field displays the user name created when you add a new user. The admin account is the default NSA super user and cannot be deleted.
Description	This field displays any configured details about the user account.

8.2.0.1 Conflict Users

A conflict user is a local user that has the same user name as that of a user on a domain controller. For example, if you first create local users and groups on the NSA (in **Workgroup** mode) and later you change to domain mode where you create (or there are already) identical users and groups, then they appear as in conflict on the NSA.

You cannot set a disk quota for users that are in conflict.

If you started in **Domain** mode and later you switch to **Workgroup** mode, the NSA will allow you to create user names and group names that already exist on the domain controller.

If the conflicting domain user's password and local user's password are NOT the same, than the two users are treated as two distinct users. Therefore, each user can only access shares to which they have been given access rights.

However, if the domain user's password and local user's password are also the same, then only shares set to be accessible by the local user are actually accessible by both the domain user and local user. The NSA has no way to distinguish these two users as their passwords and user names are exactly the same.

During a conflict situation, the local user takes precedence ONLY if the domain user and local user's passwords are the same.

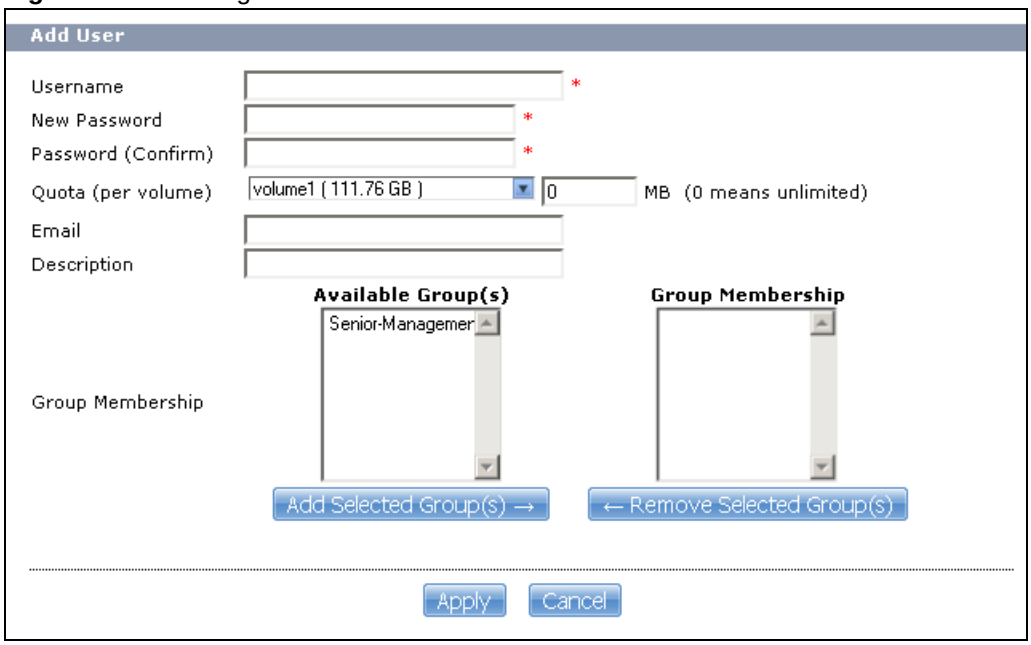
8.2.1 Create a New Account & Change Account Properties

To create an account, click **Sharing** > **Users** > **Add User**.

To edit an existing local user account, click **Sharing** > **Users** > **Edit User**.

The account creation and account editing screens are identical in appearance.

Figure 152 Sharing > Users > Add User



The following table describes the labels in this screen.

Table 51 Sharing > Users > Create a New Account

LABEL	DESCRIPTION
Username	Enter an account name.The text may consist of up to 14 letters, numerals and any printable character found on a typical English language keyboard, with certain limitations due to the nature of the NSA system. See Section 8.2.1.1 on page 179 for more details on account names.
Password	Create a password associated with this account. The text may consist of up to 14 letters, numerals and any printable character found on a typical English language keyboard.
Password (Confirm)	Enter the exact same password that you just typed in the above field.
Quota (per volume)	Set how many megabytes of storage the account can use in each of the NSA's volumes. You can set a different quota for each volume. A value of "0" MB means unlimited storage. The quota for an individual volume cannot exceed 500000000 MB (488,281 gigabytes, or 477 terabytes).
Email	Enter the user's e-mail address.
Description	Enter details about the user account. The text may consist of up to 110 letters, numerals and any printable character found on a typical English language keyboard except quotation marks (') or ('').

Table 51 Sharing > Users > Create a New Account (continued)

LABEL	DESCRIPTION
Group Membership	Choose the groups to which you want to assign this account. You can select multiple groups by holding the [Ctrl] key while you click. Before a user can be assigned a group, you must first create one or more on the NSA. A group is a set of users that have common NSA access rights. A user can belong to more than one group. More restrictive access rights override less restrictive ones.
Available Groups	These are the groups that have been created on either the NSA or the domain controller. Select the group(s) that you want the account to join and then click the **Add Selected Group(s)** button. You need to click **Apply** for the changes to take effect.
Group Membership	These are the groups that the account already belongs to on either the NSA or domain controller. Select the group(s) that you want the account to leave and then click the **Remove Selected Group(s)** button. You need to click **Apply** for the changes to take effect.
Apply	Click this to save your changes.
Cancel	Click this to discard changes and close the dialog box.

8.2.1.1 Account Names

Enter an account name from 1 to 14 characters. The first character must be alphabetical (case insensitive, [A-Z a-z]); numeric characters are not allowed as the first character.

The account name can only contain the following characters:

- Alphanumeric A-z 0-9
- Spaces
- _ [underscores]
- . [periods]
- - [dashes]

Other limitations on account names are:

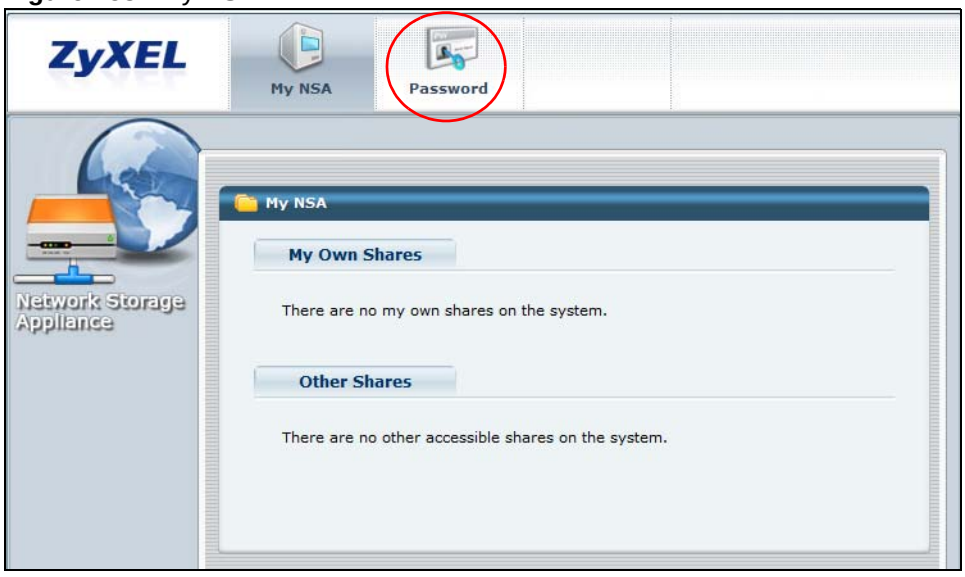
- All leading and trailing spaces are removed automatically.
- Multiple spaces within names are converted to a single space.
- Account names are case insensitive. The account name cannot be the same (regardless of the letter case) as an existing local account or domain account. For example, if there exists a domain account with the name 'BOB', you cannot create a local account named 'bob'. If you enter an account 'bob' but use 'BOB' when connecting via CIFS or FTP, it will use the account settings used for 'bob'.
- The account name cannot be the same as a system account name such as **FTP** or **EVERYONE** nor be the same as an existing local or domain account. Other reserved user names that are not allowed are:
  - bin
  - daemon
  - ftp
  - anonymous
  - nobody
  - root
  - pc-guest

- admin

8.2.1.2 Account Password Management

Non-admin users may change their passwords themselves by logging into the NSA Web Configurator using the username and password as defined in the **Create New Account** screen. After logging in, select the **Password** tab in the account toolbar.

Figure 153 My NSA



In the **Password** tab, create a new password and then click **Apply**.

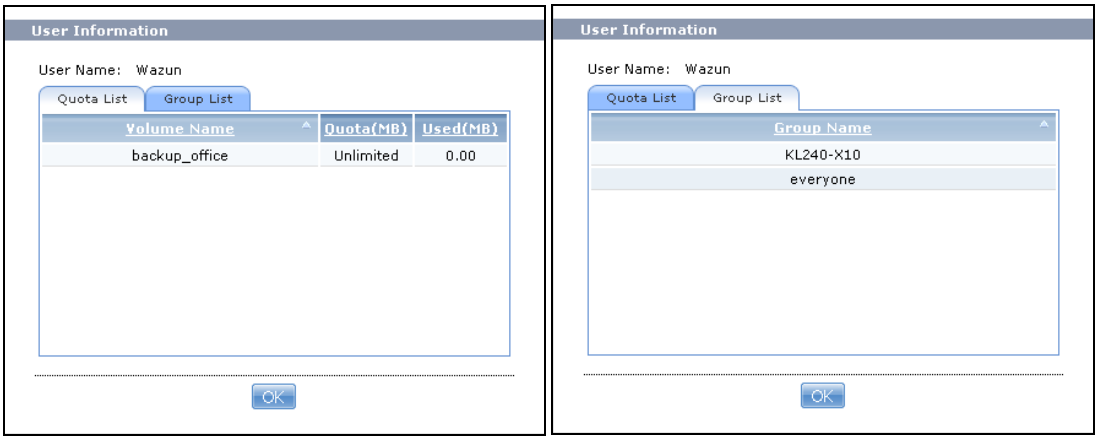
Figure 154 Password

Non-admin user accounts cannot access the administrator Web Configurator screens and cannot browse shares assigned to other users.

8.2.2 View User Information

To view a user account's information, select it from the **Sharing** > **Users** list and then click **User Info**. The two tabs in the **User Information** screen are **Quota List** and **Group List**.

Figure 155 Sharing > Users > User Information



The following table describes the labels in this screen.

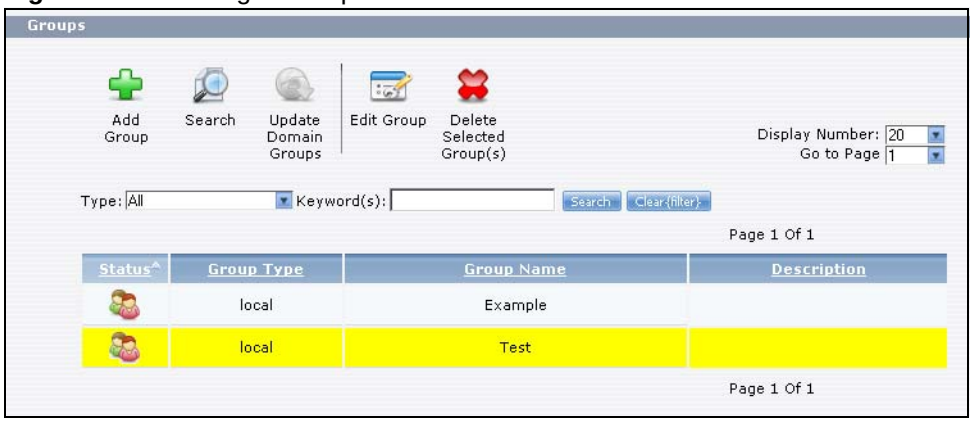
Table 52 Sharing > Users > User Information > Quota List

LABEL	DESCRIPTION
User Name	Displays the name of the selected user.
Volume Name	Displays the volume names.
Quota (MB)	Indicates the size of the selected user's volume quota in megabytes (MB).
Used (MB)	Indicates how much of the volume quota the selected user has used. Used quote is measured in megabytes (MB).
Group Name	Indicates the groups to which the selected user belongs.
OK	Click this to close the screen.

8.3 Groups

Click **Sharing** > **Groups** to open this screen where you can create and manage groups. A group is a collection of user accounts.

Figure 156 Sharing > Groups



The following table describes the icons in this screen.

Table 53 Sharing > Groups Icons

ICON	DESCRIPTION
	Add Group Click this icon to open the **Add a New Local Group** screen, where you can add new local groups. See Section 8.3.1 on page 184 for details.
	Search Click this icon to display the search filters which you can use to search for user groups by type or keyword.
	Update Domain Groups Select a group from the list, then click this icon to retrieve its domain information, where applicable.
	Edit Group Select a group from the list, then click this icon to edit its permissions. See Section 8.2.1 on page 178 for details.

Table 53 Sharing > Groups Icons (continued)

ICON	DESCRIPTION
	Delete Selected Groups Select a group from the list, then click this icon to remove it. You can only delete local user groups, not domain groups.
	Sort Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.
	Local Group Indicates a local group created on the NSA.
	Conflict Local Group Indicates a local group created on the NSA that is in conflict with a domain group.
	Domain Group Indicates a domain group created on a domain controller.
	Conflict Domain Group Indicates a domain group created on a domain controller that is in conflict with a local group created on the NSA.

The following table describes the labels in this screen.

Table 54 Sharing > Groups

LABEL	DESCRIPTION
Display Number	Set the number of groups displayed per page.
Go to Page	Select a page number of user account groups to display.
Type	This field displays when you click the **Search** icon. Use it to filter search results according to the user group type selected.
Keyword(s)	This field displays when you click the **Search** icon. Enter a specific word for which to search. The default is all words.
Search	This button displays when you click the **Search** icon. Click to begin searching according to the search parameters you set. If you choose not to set any search parameters, then the defaults for each filter is used.
Clear{filter}	This button displays when you click the **Search** icon. Click to reset all the search filters back to their default settings.

Table 54 Sharing > Groups (continued)

LABEL	DESCRIPTION
Previous & Next	Click **Previous** to cycle back through the pages of groups, and **Next** to cycle forward through them.
Status	This icon displays the type of group and can also show if the group is in conflict.
Group Type	This field displays whether the group is a local group or a domain group.
Group Name	This field displays the group name.

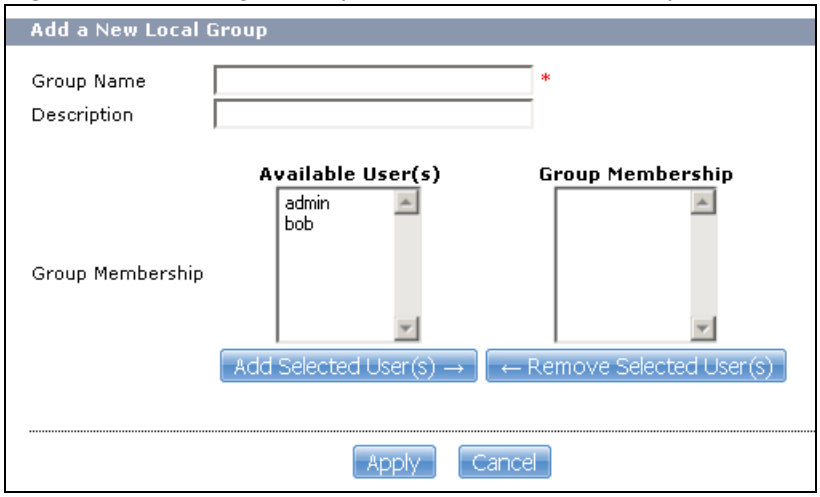
8.3.1 Add a New Local Group & Change Group Properties

To create a local group, click **Sharing** > **Groups** > **Add Group**.

To edit an existing local group, click **Sharing** > **Groups** > **Edit Group**.

The group creation and group editing screens are identical in appearance.

Figure 157 Sharing > Groups > Add a New Local Group



The following table describes the labels in this screen.

Table 55 Sharing > Groups > Add a New Local Group

LABEL	DESCRIPTION
Group Name	Enter a local group name.The text may consist of up to 16 letters, numerals and any printable character found on a typical English language keyboard, with certain limitations due to the nature of the NSA system. See Section 8.3.1.1 on page 185 for more details on account names.
Group Membership	Choose which user accounts should be added to or removed from this group. You can select multiple user accounts by holding the [Ctrl] key while you click. A group is a set of users that have common NSA access rights. A user can belong to more than one group.
Description	Enter details about the user group. The text may consist of up to 110 letters, numerals and any printable character found on a typical English language keyboard except quotation marks.

Table 55 Sharing > Groups > Add a New Local Group (continued)

LABEL	DESCRIPTION
Available Users	These are the user accounts that have been created on either the NSA or the domain controller. Select the user(s) that you want to join the group and then click the **Add Selected Users)** button. You need to click **Apply** for the changes to take effect.
Group Membership	These are the groups that the account already belongs to on the NSA. Select the group(s) that you want the user to leave and then click the **Remove Selected Group(s)** button. You need to click **Apply** for the changes to take effect.
Apply	Click this to save your changes.
Cancel	Click this to discard changes and close the dialog box.

8.3.1.1 Group Names

Enter a group name from 1 to 16 characters. The first character must be alphabetical (case insensitive, [A-Z a-z]); numeric characters are not allowed as the first character.

The group name can only contain the following characters:

- alphanumeric A-z 0-9 (there is no unicode support)
- Spaces
- _ [underscores]
- . [periods]
- - [dashes]

Other limitations on group names are:

- All leading and trailing spaces are removed automatically.
- Multiple spaces within names are converted to a single space.
- Group names are case insensitive. The group name cannot be the same (no matter the case) as an existing local group or domain group. For example, if there exists a domain group with the name 'BOB', you cannot create a local group named 'bob'. If you enter a group 'bob' but use 'BOB' when connecting via CIFS or FTP, it will use the account settings used for 'bob'.

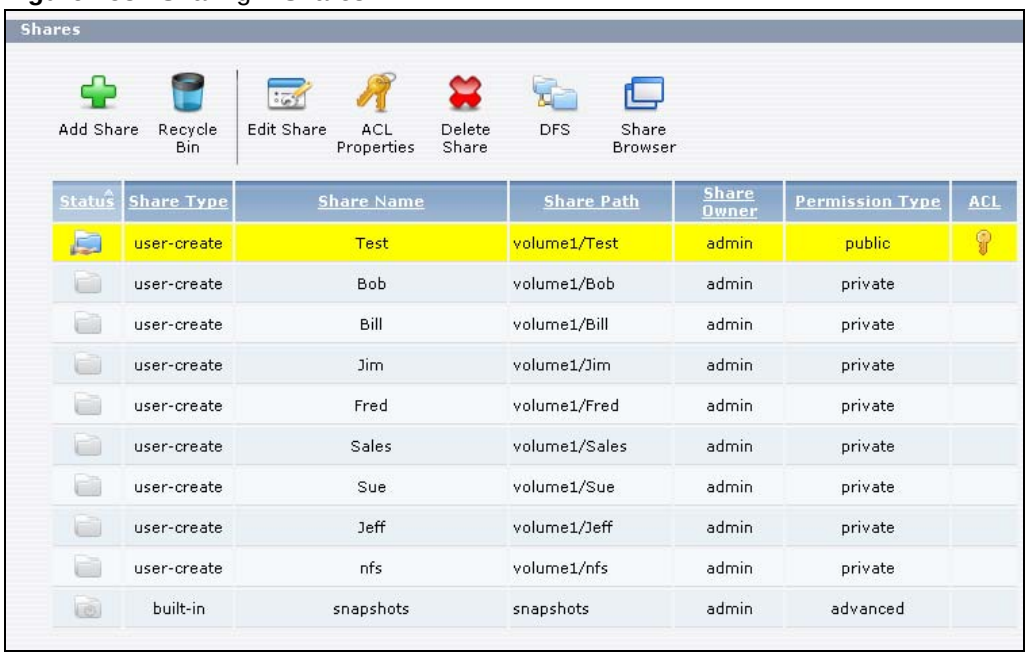
The group name cannot be **EVERYONE** nor be the same as an existing local or domain group. Other reserved group names that are not allowed are:

- daemon
- disk
- ftp
- nobody
- lp
- root
- tty
- utm

8.4 Shares

Click **Sharing** > **Shares** to open this screen where you can create and manage shares.

Figure 158 Sharing > Shares



The following table describes the icons in this screen.

Table 56 Sharing > Shares Icons

ICON	DESCRIPTION
	Add Share Click this icon to open the **Add Share** screen, where you can create new shares. See Section 8.4.1 on page 188 for details.
	Recycle Bin Click this icon to open the **Recycle Bin Configuration** screen. See Section 8.4.3 on page 194 for details.
	Change Share Properties Select a share from the list, then click this icon to edit its settings. See Section 8.4.2 on page 190 for details.
	ACL Properties Click this icon to open the **ACL Configuration** screen, where you can set up an Access Control List. See Section 8.4.2 on page 190 for details.

Table 56 Sharing > Shares Icons (continued)

ICON	DESCRIPTION
	Delete Share Select a share from the list, then click this icon to remove it.
	DFS Click this icon to open the **DFS Links** screen. See Section 8.4.4 on page 194 for details on creating DFS links.
	Share Browser Select a share from the list, then click this icon to view its folder and file structure. You can also add, remove, and move files and folders within a share. See Section 2.5.1 on page 40 for details on browsing screens.
	Sort Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.
	ACL Active Indicates that an ACL is being used to manage the files in this share.
	Available Share Indicates the share can be used for file and folder management.
	Unavailable Share Indicates the share cannot be used because the NSA cannot find the physical location of the share.
	Disabled Share Indicates the share is no longer functional. If this happens, talk to your network administrator.

The following table describes the labels in this screen.

Table 57 Sharing > Shares

LABEL	DESCRIPTION
Status	This icon displays whether the share is available, unavailable or disabled. The default and snapshot shares cannot be deleted.
Share Type	This displays whether the share is created by the system or by an administrator account.
Share Name	This displays the name of the shared folder on the NSA.
Share Owner	This displays the name of the user account that owns the share.
Permission Type	This displays the type of permissions assigned to the share. Options are public, private, and advanced.
ACL	The key icon indicates that a share has an Access Control List.

Table 57 Sharing > Shares (continued)

LABEL	DESCRIPTION
Display Number	Set the number of shares displayed per page.
Previous & Next	Click **Previous** to cycle back through the pages of shares, and **Next** to cycle forward through them.

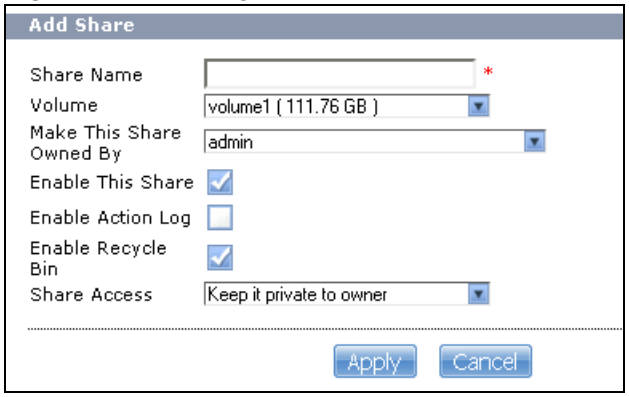
8.4.1 Create a New Share & Edit a Share

To create a local group, click **Sharing** > **Shares** > **Add Share**.

To edit an existing local group, click **Sharing** > **Shares** > **Edit Share**.

The share creation and share editing screens are identical in appearance.

Figure 159 Sharing > Shares > Create a New Share



The following table describes the labels in this screen.

Table 58 Sharing > Shares > Create a New Share

LABEL	DESCRIPTION
Share Name	Enter the name of the shared folder. The text may consist of 1 to 255 characters. See Appendix on page 44
Volume	Select a volume for the share to be located on.
Make This Share Owned By	Select an owner for the share.
Enable This Share	Select this to activate the share.
Enable Action Log	Select to keep a log of all actions performed on files/folders in the share. These actions include whenever anyone adds or removes a folder, and reads, writes, or deletes a file.
Enable Recycle Bin	Select this to create a recycle bin on the share. Whenever a user with sufficient permissions deletes a file or folder, it is stored here until it can be deleted permanently. By default, the recycle bin is enabled. This ensures that any inadvertently deleted data can be recovered. Because the NSA file system uses XFS, the data recovery depends on the system administrator's use of a volume manager. As such, this feature is enabled automatically until explicitly disabled in order to facilitate file restoration should the need arise. Be sure to use the recycle bin configuration screen (Section 8.4.3 on page 194) to clear out the recycle bin periodically or else its host volume will fill up and users will not be able to store any new files on it.
Share Access	Choose whether the share is public or private, or choose **Advanced** to open the **Share Access Configuration** screen.

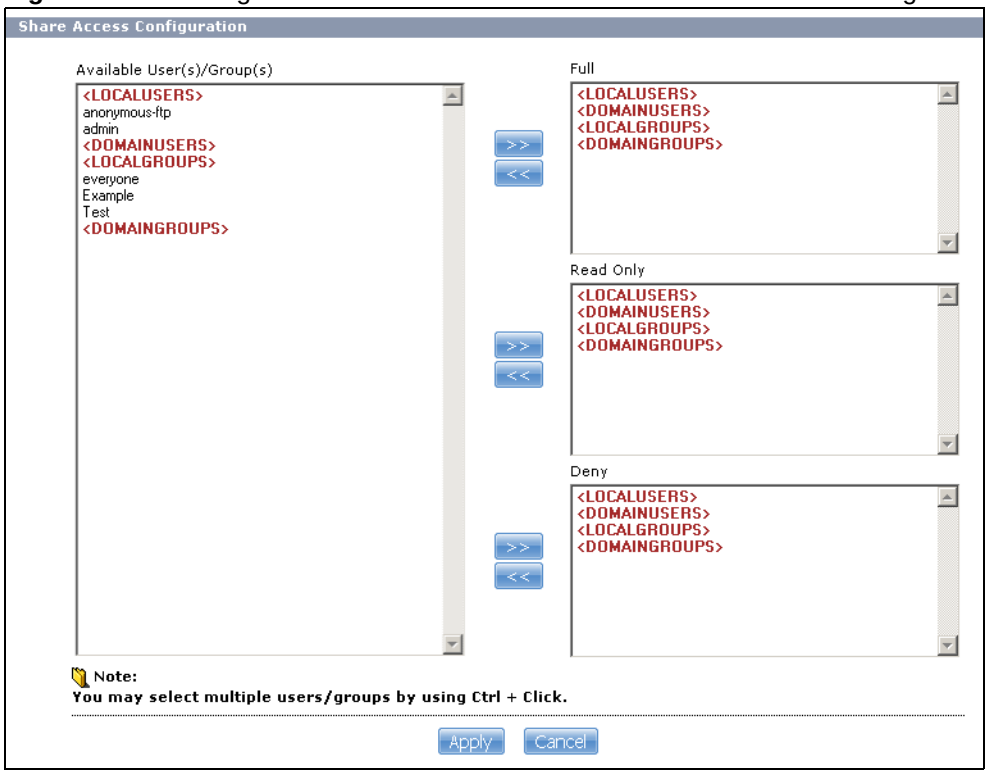
Table 58 Sharing > Shares > Create a New Share (continued)

LABEL	DESCRIPTION
Apply	Click this to save your changes.
Cancel	Click this to discard changes and close the window.

8.4.1.1 Share Access Configuration

This screen allows you to assign permissions to a share.

Figure 160 Sharing > Shares > Create a New Share > Share Access Configuration



The following table describes the labels in this screen.

Table 59 Sharing > Shares > Create a New Share > Share Access Configuration

LABEL	DESCRIPTION
Available Users/Groups	This displays a list of users and groups that have not yet been assigned an authority level for the share. You can assign users and groups by selecting them and clicking the right arrow.
Full Read Only Deny	Assign users and groups one of the following authority levels. **Full** - Grants read/write privileges. **Read Only** - Grants read-only privileges; files and folders cannot be modified, moved, or removed. **Deny** - Removes all privileges; files and folders cannot be read, modified, moved, or removed. You can remove users from any given authority level by selecting them and clicking the left arrow.
Apply	Click this to save your changes.
Cancel	Click this to discard changes and close the window.

8.4.2 ACL Configuration

Click **Sharing** > **Shares**, select a share, and click **ACL Properties** screen to open the Access Control List (ACL) screen. Use this screen to display and configure ACL settings. The ACL defines read and write permissions for specific files and folders.

- If you add a new file to a folder, the new file takes on the folder's ACL settings.
- If you move a file from one folder to another, the file keeps its ACL settings. The NSA automatically creates a new ACL for the individual file with its ACL settings.
- Copying and pasting a file from one folder to another is treated the same as creating a new file; the new file takes on the folder's ACL settings.

Figure 161 Sharing > Shares > ACL Configuration

The following table describes the icons in this screen.

Table 60 Sharing > ACL Configuration Icons

ICON	DESCRIPTION
	New ACL Click this icon to open the **New ACL Configuration** screen. See Section 8.4.2.1 on page 191 for details.
	Modify ACL Click this icon to open the **ACL Permission** screen. See Section 8.4.2.2 on page 192 for details.
	Reset ACL Click this to reset the ACL permissions on the selected file or folder.
	Restricted Folder This is a folder that has ACL permissions set.
	Restricted File This is a file that has ACL permissions set.

The following table describes the labels in this screen.

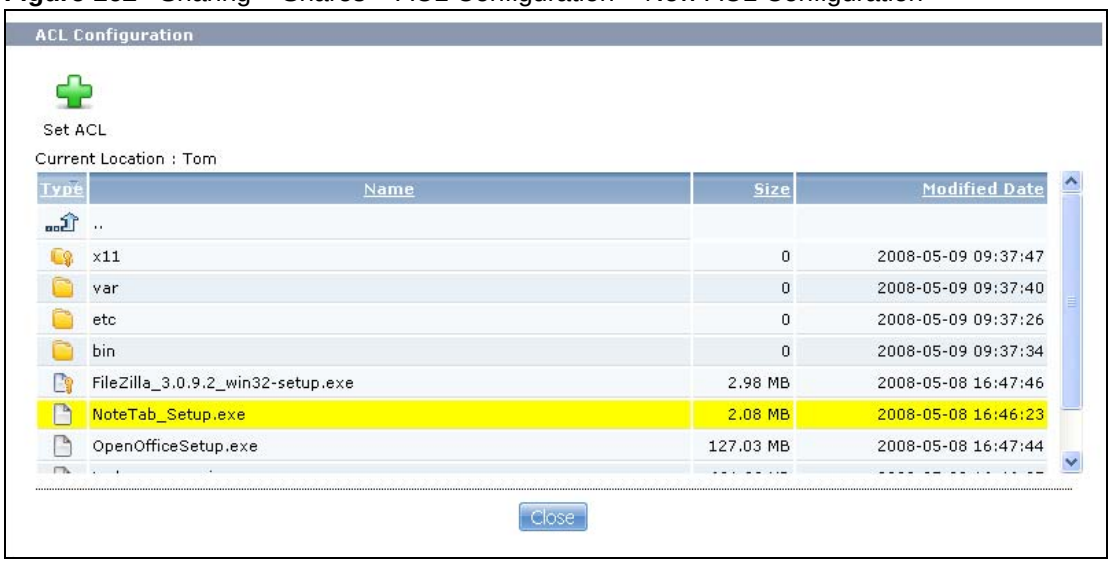
Table 61 Sharing > Shares > Create a New Share > Share Access Configuration

LABEL	DESCRIPTION
Type	This indicates whether the item in the list is a folder or file, as well as whether it is locked or unlocked.
ACL Path	This indicates the file or folder path and name on the share.
Close	Click this to close the screen.

8.4.2.1 New ACL Configuration

This screen allows you to create a new ACL configuration.

Figure 162 Sharing > Shares > ACL Configuration > New ACL Configuration



The following table describes the icons in this screen.

Table 62 Sharing > Shares > ACL Configuration > New ACL Configuration Icons

ICON	DESCRIPTION
	Set ACL Select a file or folder from the list, then Click this icon to open the **ACL Permission** screen. See Section 8.4.2.2 on page 192 for details.
	Unrestricted Folder This is a folder that has no ACL permission set.
	Restricted Folder This is a folder that has ACL permissions set.
	Unrestricted File This is a file that has no ACL permissions set.
	Restricted File This is a file that has its ACL permissions set.

The following table describes the labels in this screen.

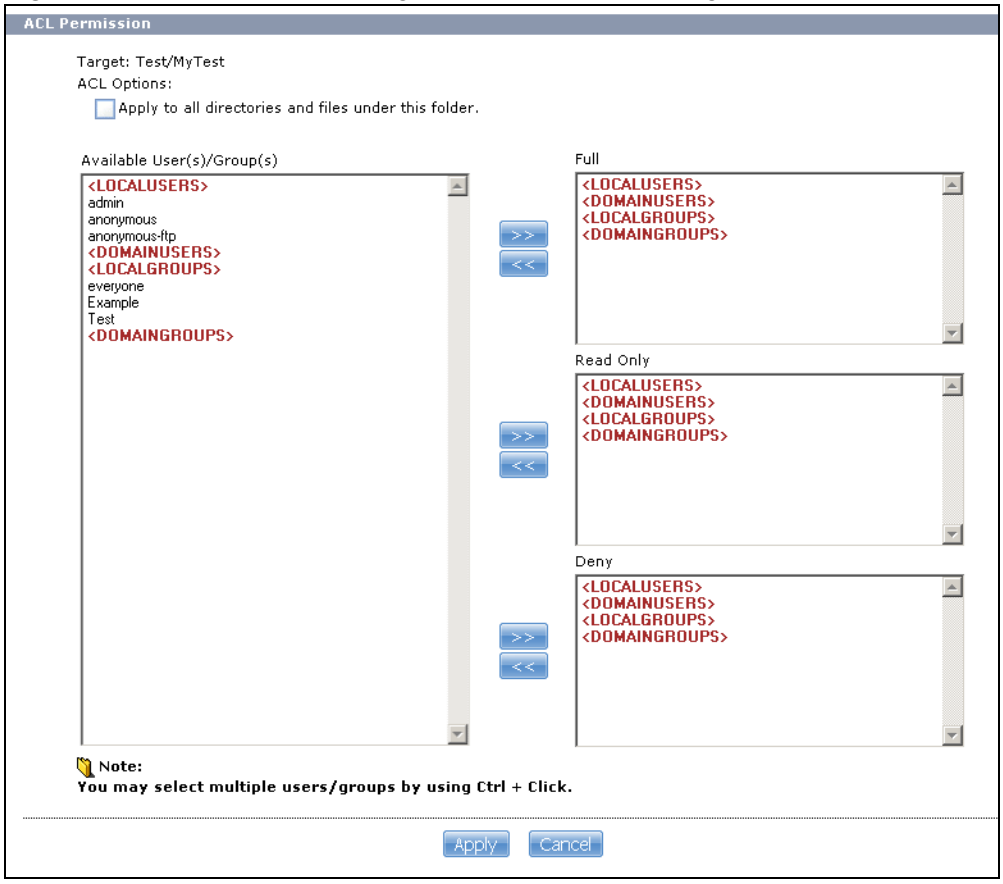
Table 63 Sharing > Shares > Create a New Share > Share Access Configuration

LABEL	DESCRIPTION
Type	This indicates whether the item in the list is a folder or file, as well as whether it is locked or unlocked.
Name	This indicates the file or folder's name on the share.
Size	This indicates the file or folder's size on the share in kilobytes.
Modified Date	This indicates when the file or folder was last altered on the share. When a file is uploaded to the NSA that is classified as a "modification" as it is considered newly written data by the device.
Close	Click this to close the screen.

8.4.2.2 ACL Permissions

Use this screen to set who can access the selected folder or file.

Figure 163 Shares > ACL Configuration > New ACL Configuration > ACL Permission



The following table describes the labels in this screen.

Table 64 Shares > ACL Configuration > New ACL Configuration > ACL Permission

LABEL	DESCRIPTION
Target	This displays the path of the currently selected item on the share.
Apply to all directories and files under this folder	If you are configuring a folder's permission settings, select this option to have these permission settings overwrite any ACL settings of all folders and files within the folder. If you clear this option, the NSA still applies the permission settings to any directories and files under this folder that do not have other ACL settings. You can still change the ACL settings of the folder's contents later. If someone is already connected to a file or folder, changing the ACL settings does not end their current setting, but will apply to any future attempts to access the file or folder.
Available Users/Groups	This displays a list of users and groups that have not yet been assigned an authority level for the share. You can assign users and groups an authority level by selecting them and clicking the right arrow.
Full Read Only Deny	Assign users and groups one of the following authority levels. **Full** - Grants read/write privileges. **Read Only** - Grants read-only privileges; files and folders cannot be modified, moved, or removed. **Deny** - Removes all privileges; files and folders cannot be read, modified, moved, or removed. You can remove users from any given authority level by selecting them and clicking the left arrow.
Apply	Click this to save your changes.
Cancel	Click this to discard changes and close the window.

8.4.2.3 EVERYONE & ANONYMOUS Share Access Rights

With an **EVERYONE** access right, you still need to log in. Every local user with an account on the NSA can access this share using their username and password. Users with accounts on a domain server cannot access shares with **EVERYONE** access rights. **EVERYONE** has every local user as a member. It does NOT include domain users.

With **ANONYMOUS FTP**, you must enter either 'anonymous' or 'ftp' as the user name. Any other name is considered a user name, so must be valid and have a corresponding correct password.

If you are already logged into a share using your username and password, you will NOT be able to access a share that has **ANONYMOUS FTP** only access rights, as these require 'no login'. If this is not your intention, it is recommended you set **EVERYONE** AND **ANONYMOUS FTP** access rights to these type shares.

See Section 8.4.2.2 on page 192 for details on permissions.

8.4.3 Recycle Bin

Click **Sharing** > **Shares** > **Recycle Bin** to open the following screen. Use this screen to set up how the share recycle bin is managed.

Figure 164 Sharing > Shares > Configuration

Recycle Bin Configuration
Clean Recycle Bin every 0 days (0~31, 0 means not clean it automatically.)
Empty ALL Recycle Bins Now
Apply
Cancel

The following table describes the labels in this screen.

Table 65 Shares > ACL Configuration > New ACL Configuration > ACL Permission

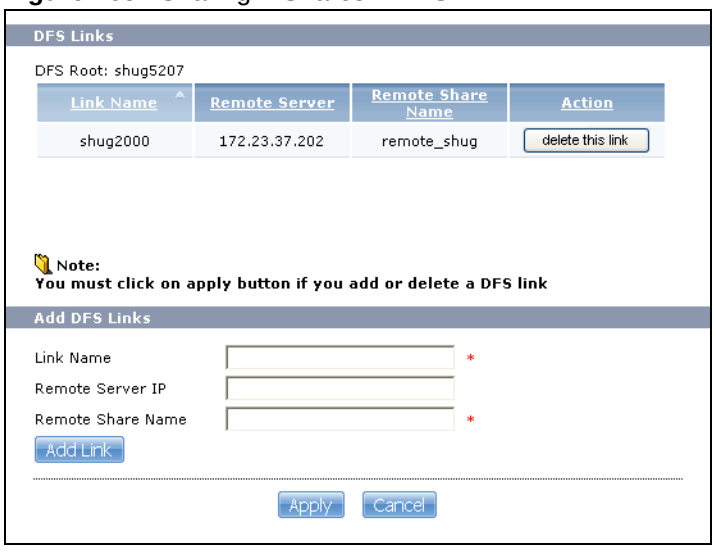
LABEL	DESCRIPTION
Clean Recycle Bin every...	Set the number of days a deleted file can remain in the recycle bin before the NSA permanently deletes it. If you enter a value of “0” then it never automatically cleans out the recycle bin and you must clean it manually.
Empty All Recycle Bins Now	Click this button to manually delete all files and folders from all of the shares’ recycle bins.
Apply	Click this to save your changes.
Cancel	Click this to discard changes and close the window.

8.4.4 DFS

Distributed File System (DFS) is a network server component that makes it easier for you to find and manage data on your network. Through DFS, you can build a single hierarchical file system whose contents are distributed throughout your organization’s network. It permits shares to be hierarchically connected to other Windows shares. Since DFS is a logical mapping, the physical location of data becomes transparent to your users and applications.

You can use DFS links when accessing the NSA using CIFS, not FTP.

Figure 165 Sharing > Shares > DFS



The following table describes the labels in this screen.

Table 66 Sharing > Shares > DFS

LABEL	DESCRIPTION
Link Name	Enter a name for the new DFS link. The text may consist of letters, numerals and any printable character found on a typical English language keyboard.
Remote Server IP	Enter the remote server's IP address.
Remote Share Name	Enter a name for the new remote share. The text may consist of letters, numerals and any printable character found on a typical English language keyboard
Add Link	Click this button to add the information in **Add DFS Links** to the list.
Delete This Link	Click this button to permanently remove the associated DFS link.
Apply	Click this to save your changes.
Cancel	Click this to discard changes and close the window.

9

Protect Screens

9.1 Protection Methods Overview

This chapter introduces different ways of protecting data on the NSA and explains how to use the **Protect** screens to create and schedule snapshots and backups.

There are a variety of ways to protect your data on the NSA. Below is a summary table of preventative steps you should do in advance to protect against various problems.

Table 67 Protection Methods Overview

PROBLEM	RECOMMENDED PREVENTATIVE ACTION
Unexpected NSA behavior after configuration changes	Back up the NSA configuration file before you make major configuration changes.
(On Your Computer) Corrupt data files Data infected by virus Data files incorrectly deleted or modified	Use the Genie Backup Manager. Use anti-virus software on your computer.
(On the NSA) Corrupt data files Data infected by virus Data files incorrectly deleted or modified	Create regular snapshots (recommended for volumes with data that changes often). Use anti-virus software on your computer to scan files from others before saving them on the NSA. You can also use anti-virus software on your computer to scan the NSA for viruses.
(On the NSA) Hard drive malfunction.	Use RAID.
NSA malfunction Network down Natural disaster such as a fire or earthquake occurs where your NSA is located	Back up data to another NSA or computer or an external USB hard drive.
Hacking	Place the NSA behind a hardware-based firewall. Ideally the firewall should include deep packet inspection, IDP (Intrusion Detection and Prevention), and anti-virus (like ZyXEL's ZyWALL USG products for example). Configure strong user passwords and Access Control List (ACL) settings. See Chapter 8 on page 173 for details. Use HTTPS for Web Configurator access to the NSA (see Section 11.4 on page 239).
Theft of files by removing the physical hard drives.	Store sensitive data in encrypted NSA volumes (see page Encrypted Volumes on page 126).

9.1.1 What You Can Do in the Protect Screens

- Use the **Backup** screens (Section 9.2 on page 200) to back up data and restore backup files by archive backup job.
- Use the **Restore** screens (Section 9.3 on page 212) to restore by backup files.
- Use the **Snapshot** screens (Section 9.4 on page 215) to create and manage snapshot jobs.
- Use the **Backup Software** screen (Section 9.5 on page 220) to locate the Genie Backup Manager license keys.

9.1.2 What You Need to Know About Protection Methods

Configuration File Backup and Restoration

Use the **Maintenance** > **Configuration** menus to create a file of your NSA configurations such as passwords, shares and volumes created, network settings and so on. If you're going to do some major configuration changes, then it is advisable to create a configuration backup file. If things go wrong after you make the configuration changes, you can always go back to the previous configuration by restoring an earlier configuration file.

If you forgot the NSA password, then reset the device to go back to the factory default configuration.

Configuration File Backup and Restoration does not affect disk arrays, volumes, or data (your files and folders) on the NSA.

Genie Backup Manager

Use the Genie Backup Manager to transfer data from your computer to the NSA. You could use Genie Backup Manager to back up from one NSA to another NSA but it's recommended you use the NSA **Protect** > **Backup** to do this (see Section 9.2 on page 200) as the latter would be faster.

The Genie Backup program uses the same network port as the NDU to discover the NSA. To avoid a port conflict, do not run the Genie Backup Manager at the same time as the NDU.

Snapshots

A snapshot is a record of changes to an internal volume at a particular moment in time. As it only records changes to files made in a volume, it's faster and takes up less space than a backup. Snapshots are good for data that changes often and needs to have high availability. If files within a volume become infected or corrupted, you can revert files back to their state at a snapshot.

You create snapshots of a complete volume, not a single file or folder within a volume.

To use a snapshot to restore files, use the MyNSA screens, CIFS (Windows Explorer), or FTP to browse to the snapshot image folder. The snapshot folder contains images named after the folders and files in the volume at the time of the backup. To restore a folder or file to its state at the time of the snapshot, open the snapshot image of the same name. You can also copy or move the snapshot image to another folder (outside the snapshot folder).

When you use a snapshot to restore files, the NSA keeps intermediate snapshots between the snapshot you use and the present. For example, say you had the NSA take daily snapshots and on Friday you choose to use Monday's snapshot; the NSA keeps the Tuesday, Wednesday, and Thursday snapshots.

Although you can continue to work while the NSA takes a snapshot, it's a good idea to schedule snapshots for non-peak times so not very many files are open. Snapshots may get progressively slower as more are done but they are still very fast compared to backups (as only block changes are recorded).

The NSA automatically purges snapshots.

See Snapshot Purging on page 215 for details.

Snapshots Versus Backups

See Section 9.2 on page 200 for more information on backups.

1. A snapshot only records changes to files within a volume, so it’s faster and takes up less space than a backup.
2. You must create a snapshot of a complete volume, not on a single file or folder as you can do with a backup.

It’s a good idea to take both snapshots and backups for the following reasons:

1. Snapshots may become invalid, so it’s good to also have backups available in case that happens. Backups are more reliable than snapshots.
2. Backups are more reliable than snapshots. So have backups available in case snapshots become invalid.
3. Backups may require several hours depending on the amount of data you have to back up (it’s a good idea to schedule backups at non-peak times), so you should take a snapshot of your data before the backup is run. If a file becomes corrupt during the backup, you can still revert to the previous snapshot and back up again.
4. If files to be backed up are open at the time of the backup, then make sure that snapshots are allowed. If they are allowed and files are open at the time the backup is run, then backup first takes a snapshot and then copies the files from this snapshot.

A backup proceeds without the snapshot if there is not enough space for the snapshot, but if an open file changes during the backup, the backup fails.

Finding Out More

See Chapter 6 on page 125 for more information on RAID.

See Section 3.7 on page 89 for backup and snapshot tutorials.

9.2 NSA Backup Screens

Use the **Protect** > **Backup** menus to create data backups to another volume, an external USB disk drive, or a computer or another NSA over the network.

The NSA deletes old backups according to the backup job's purge policy (see Section 9.2.2 on page 202) before creating a new backup. If you have a backup scheduled to begin at midnight, then at that time, the NSA deletes files according to the purge policy setting before doing the back up. If space on the backup NSA is a concern, then configure the NSA to delete old backups.

After purging old backups, the NSA does not check if enough space is available before backup commences. The NSA starts transferring files and if not enough space is available, it issues a log or alert to tell you that the backup failed (due to lack of space) and deletes any files already transferred.

A full backup copies all files from your NSA to the backup device. It may take some time depending on how many files you have to back up.

See also this related information:

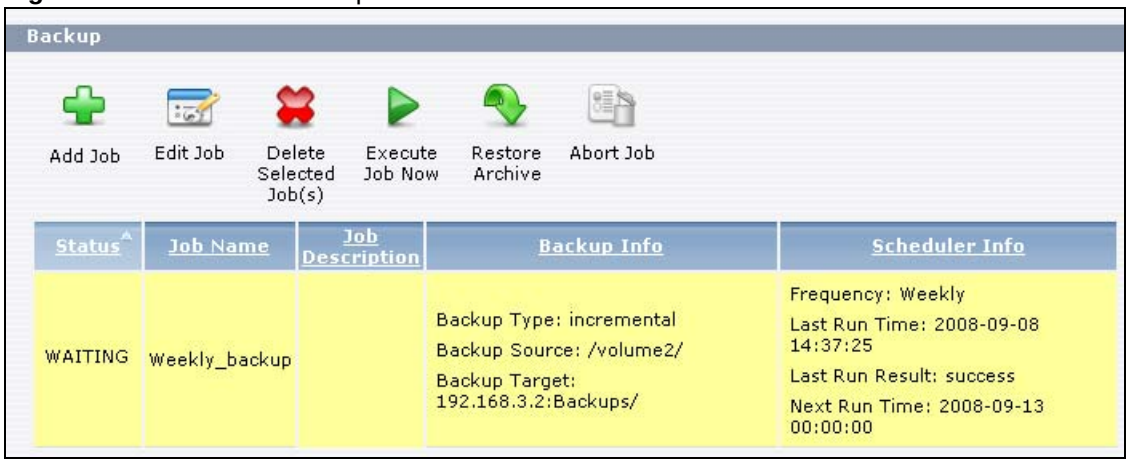
- Snapshots Versus Backups on page 199 for a comparison of backups and snapshots.
- Section 6.9.8 on page 156 for a comparison of backups and RAID.
- Section 9.1 on page 197 for an overview of protection methods available on the NSA.

To best protect data, back up data to another NSA or computer or an external hard drive, and store in an off site location.

9.2.1 Backup Summary

Click the **Backup** link in the Navigation panel to access the **Protect** > **Backup summary** screen. This screen shows a list of all backup jobs created and scheduled. You can also edit or delete an existing backups or create a new one from here. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 166 Protect > Backup



The following table describes the icons in this screen.

Table 68 Protect > Backup Icons

ICON	DESCRIPTION
	Add Job Click this icon to create a new backup job (see also Section 9.2.2 on page 202).
	Edit Job Select a backup job and click this icon to modify it's settings.
	Delete Selected Jobs(s) Select a backup job(s) and click this icon to remove the job(s). This does not delete any backup files the backup job has already created.
	Execute Job Now Select a backup job and click this icon to have the NSA perform the backup now (without waiting for the scheduled time).
	Restore Archive Select an archive backup job that has already run and click this icon to restore a previous backup from another NSA or external USB hard drive connected to the NSA. Another option is to use **Protect > Restore** (Section 9.2.3 on page 208) to restore by the backup files themselves.

Table 68 Protect > Backup Icons (continued)

ICON	DESCRIPTION
	Abort Job If a backup job is currently running, you can select it and click this icon to stop and abort the job.
	Sort Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

The following table describes the labels in this screen.

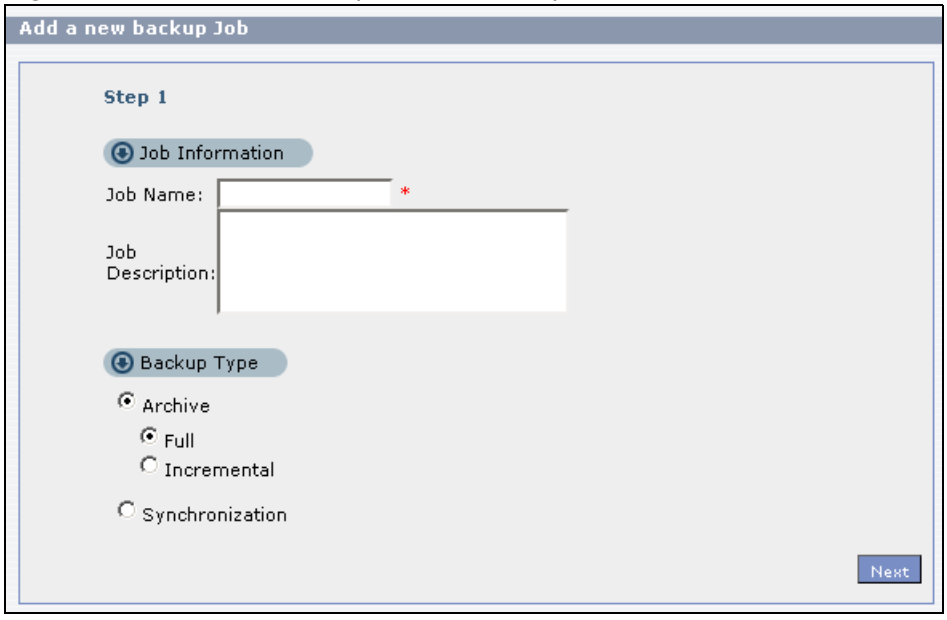
Table 69 Protect > Backup

LABEL	DESCRIPTION
Status	This field shows whether the backup job is currently running or waiting to run. The percent complete also displays for a currently running job.
Job Name	This is the name of the backup.
Job Description	This is some extra descriptive text on the backup.
Backup Info	This field displays the backup's type, source, and target.
Scheduler Info	This field displays the backup's frequency, the time it was last run in (and whether or not it succeeded), and when it is scheduled to run again. The times use yyyy-mm-dd hh:mm:ss format.

9.2.2 Creating a Backup Job

In the **Protect** > **Backup** screen, click the **Add Job** icon to create a new backup job.

Figure 167 Protect > Backup > Add Job: Step 1



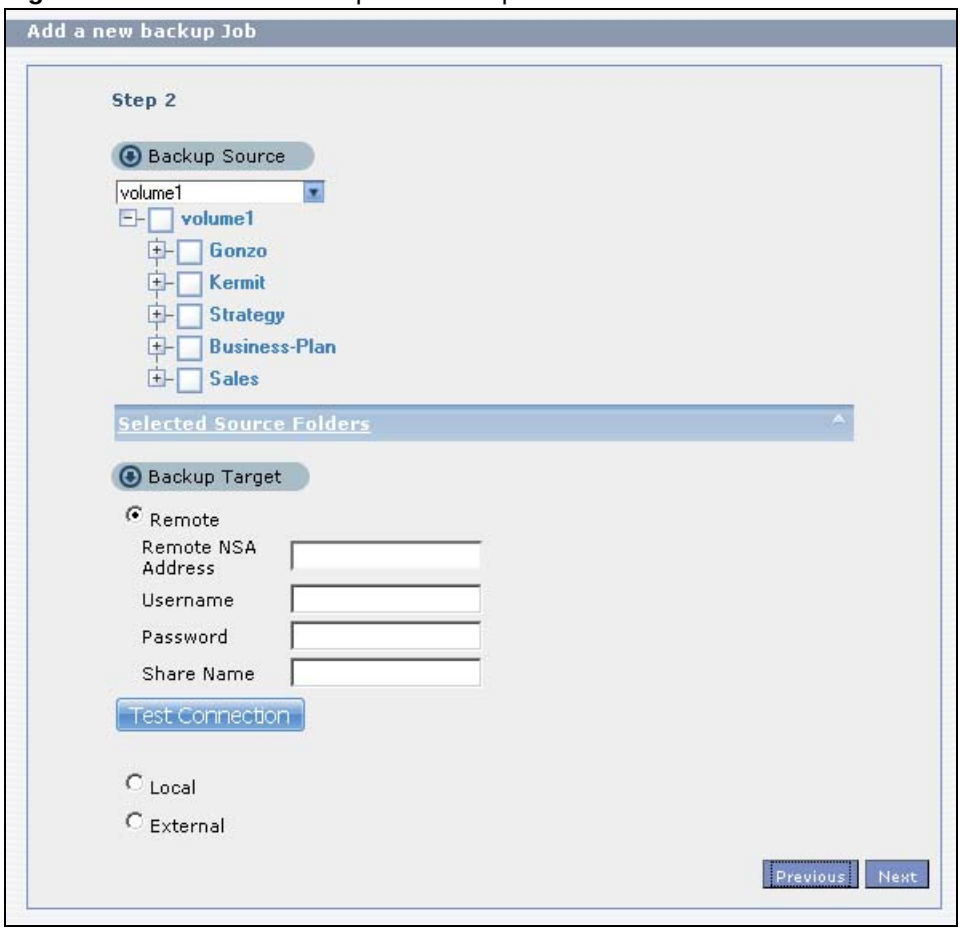
The following table describes the labels in this screen.

Table 70 Protect > Backup > Add Job: Step 1

LABEL	DESCRIPTION
Job Name	This is a required field that uniquely identifies the backup. Type from 1 to 15 characters. You can use alphanumeric characters (A-Z 0-9) and "_" [underscores]. The first character must be a letter.
Job Description	Type from 0 to 60 characters to further describe this backup.
Archive	Select this to make a separate copy of the source files for each backup. The backup copy can be on this NSA, another NSA, or a computer that uses CIFS. **Full** copies all of the source files at each backup. This provides the most protection but also requires the most storage space. **Incremental** copies only source files that are new and/or modified since the last backup. The first backup is a full backup. The NSA also does a full backup at the backup interval you specify. You can manually delete backup files, but you must keep the latest full backup to be able to restore the files later.
Synchronization	Select this to keep updating a single copy of the source files to the target. At the time of writing the target must be another NSA-2401. **Publish** makes a copy of the source files. Additional files in the target folder can remain. **Mirror** makes the target folder identical to the source folder. The NSA deletes any other files in the target folder.
Next	Click this button to proceed.

9.2.2.1 Creating a Backup Job: Step 2

Figure 168 Protect > Backup > Add: Step 2



The following table describes the labels in this screen.

Table 71 Protect > Backup > Add Job: Step 2

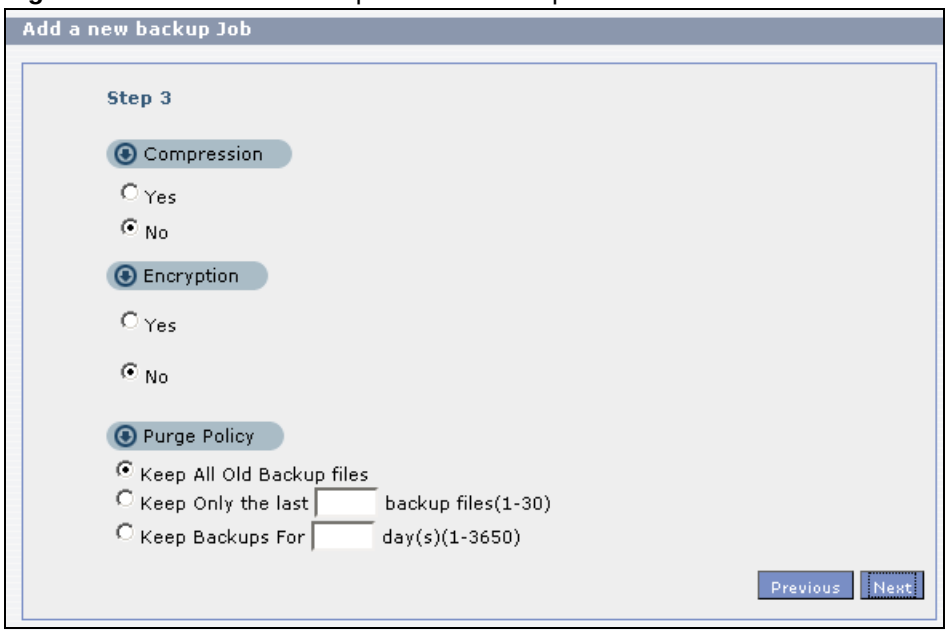
LABEL	DESCRIPTION
Backup Source	Select an (internal) volume and the folders and files to back up using this tree interface. Click + to browse through folders, sub-folders and files. Click − to close a folder in the tree. This is useful if there are many folders or files that you wish to hide from view. Click ☐ to select a folder or file to back up. This also selects all sub-folders and files. Click ☑ to deselect the folder or file. This also de.selects all sub-folders and files. More ... ▲ and More ... ▼ appear when there are too many folders/files to display. Click the arrows to scroll up or down through the folders/files. ☑ for a folder means all sub-folders and files and new folders/files added later will be backed up. ☑ for a file means the file will be backed up. ☑ (a grayed out check box) for a folder means that only some sub-folders and files under the folder will be backed up. Newly added folders/files will NOT be backed up. means the file structure is still loading. Please wait for the folders/files to display. Note: If you select to back up an entire folder ☑ and then de-select a sub-folder or file within that folder, the main folder icon will turn ☑ and any new sub-folders and files added to this main folder after the initial backup configuration will **NOT** be backed up. A list of your select folders and files displays below the selection fields.
Backup Target	Choose where to save the backup.
Remote	Select this to back up to another device. For Archives: The remote device can be another NSA or a computer that supports CIFS. Fill in the following fields in order to be able to access it. • Remote NSA Address • Username • Password • Share Name Click **Test Connection** to see if your NSA can communicate with the remote device. For Synchronization: The remote device must be another NSA compatible with the NSA's synchronization feature. Fill in the following fields in order to be able to access it. • Remote NSA Address • Username • Remote Admin's Password Click **Show target content** to connect to the remote NSA so you can select the target share for the backup.
Local	Select this to back up the files to another volume on the NSA. Select the folder where you want to store the backup files. It is recommended that the target be on a different disk array from the source volume to provide protection in the event that the source drive fails.

Table 71 Protect > Backup > Add Job: Step 2 (continued)

LABEL	DESCRIPTION
External	If there is an external USB hard drive connected to the NSA (for example USB1 ExtVolume 1), you can select a backup target on the external USB hard drive.
Previous	Click this button to return to the preceding screen.
Next	Click this button to proceed.

9.2.2.2 Creating a Backup Job: Step 3

Figure 169 Protect > Backup > Add Job: Step 3



The following table describes the labels in this screen.

Table 72 Protect > Backup > Add Job: Step 3

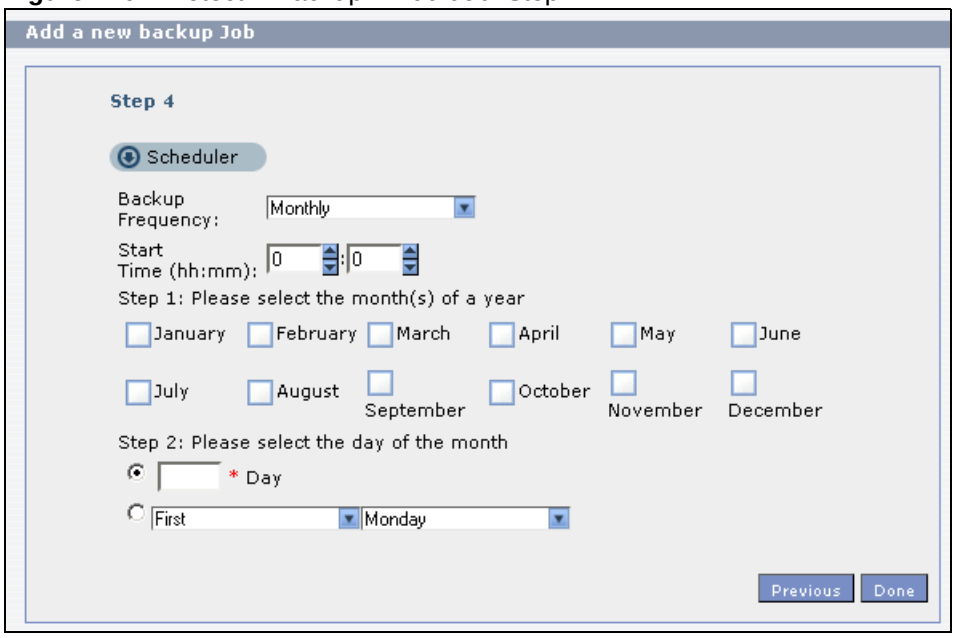
LABEL	DESCRIPTION
Compression	Compression reduces the size of the file that you want to back up although it also consumes more of the NSA's CPU's computing power. With compression enabled, the transfer of the backup file is faster. However restoring may be slower. If backup space is not a concern and recovery speed is, then turn off compression. If the backup target is at a remote site to which the NSA connects through a low bandwidth connection, turn on compression.
Encryption	For synchronization backups, enable encryption to use encryption while transferring the file. However the final file stored on the remote NSA is unencrypted. For archive backups, use encryption to create password-encrypted backup files.
Bandwidth	Restrict the bandwidth of synchronization backups to help stop them from using all of your network connection's available bandwidth. This is more important when backing up to a remote NSA or computer through the Internet.

Table 72 Protect > Backup > Add Job: Step 3 (continued)

LABEL	DESCRIPTION
Purge Policy	Select a policy for deleting archive backups. This purge runs first before a new backup is done. For example, if you have a backup scheduled to begin at midnight, then at that time, the NSA checks these settings and deletes files accordingly before backup takes place. If space on the backup NSA or disk is a concern, then configure the NSA to delete old backups. • **Keep All Old Backup files**: Purge is in effect disabled. Select this if backup space is not a concern. • **Keep Only ___ backups**: All backup files older than the last one are deleted. You will not be able to recover files that existed (only) in those previous backups. Select this if backup space is limited and recovery of old files is not important. • **Keep Backups for ___ day(s)**: Backups older than the number of days you enter here are deleted. 0 days means that all old backups are deleted when a new one is done.
previous	Click this button to return to the preceding screen.
next	Click this button to proceed.

9.2.2.3 Creating a Backup Job: Step 4

Figure 170 Protect > Backup > Add Job: Step 4



The following table describes the labels in this screen.

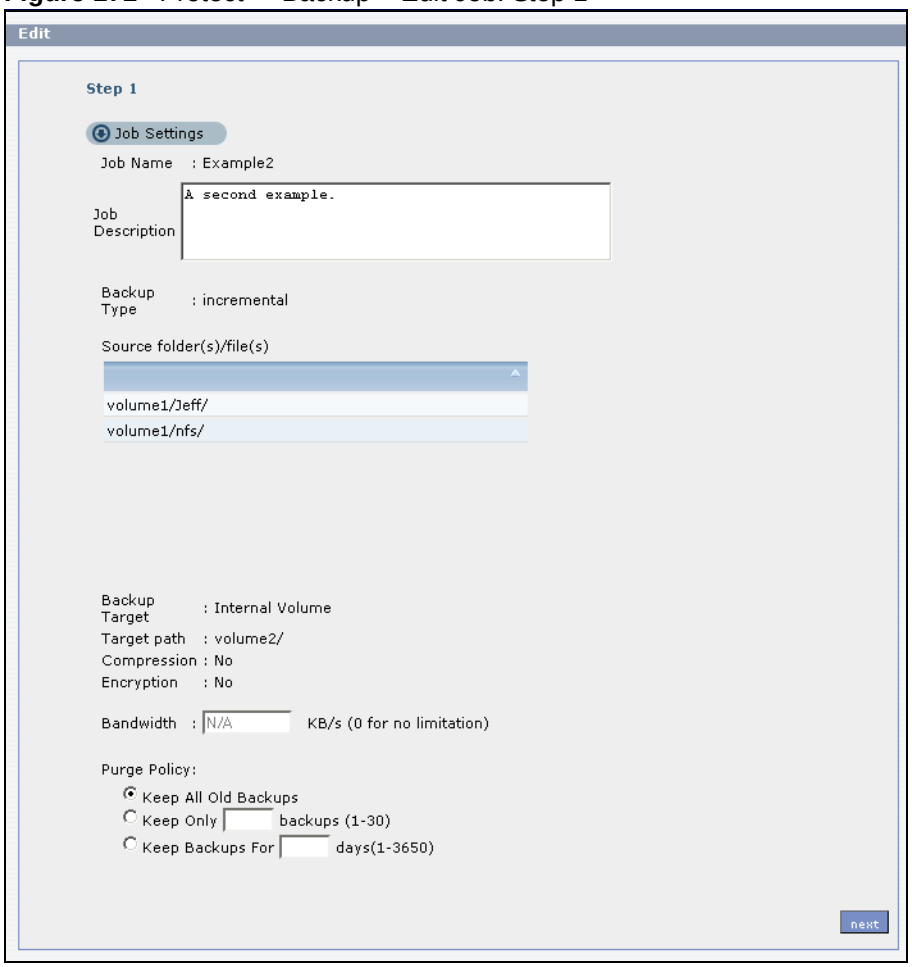
Table 73 Protect > Backup > Add Job: Step 4

LABEL	DESCRIPTION
Backup Frequency	Select how often the job should run (**Hourly**, **Daily**, **Weekly**, or **Monthly**). It is recommended you schedule large backups for times when your network is not busy, such as at night. If two events are configured to run at the same time, then one must wait until the other finishes running.
Time	Enter the time, day and/or month as appropriate for your selection above.
previous	Click this button to return to the preceding screen.
done	Click this button to save your changes.

9.2.3 Editing a Backup Job

In the **Protect** > **Backup** screen, select a backup job and click the **Edit Job** icon to change its settings.

Figure 171 Protect > Backup > Edit Job: Step 1



The following table describes the labels in this screen.

Table 74 Protect > Backup > Edit Job: Step 1

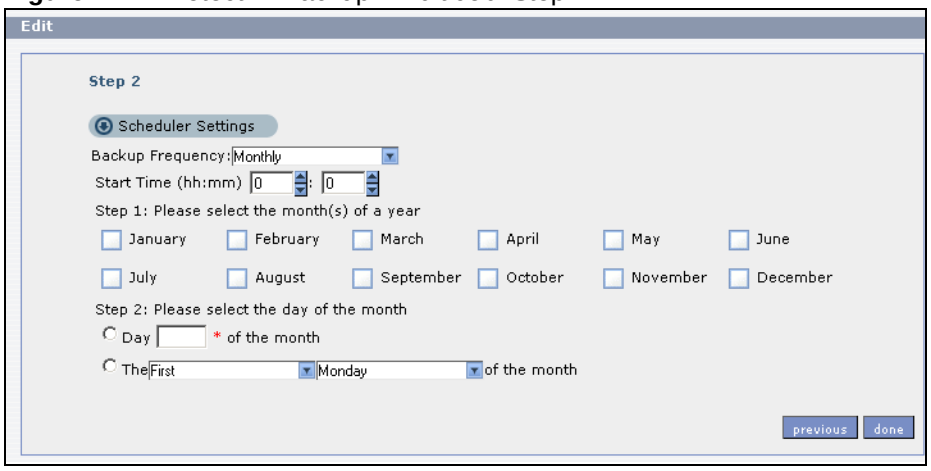
LABEL	DESCRIPTION
Job Name	This field displays the name that uniquely identifies the backup. It is read-only.
Job Description	Type from 0 to 60 characters to further describe this backup.
Backup Type	This field displays what kind of backup is to be performed. It is read-only.
Source folder(s)/file(s)	Specify the path of the folders and files to back up.
Backup Target Target path	These fields display where the backups are to be saved to.
Compression	Compression reduces the size of the file that you want to back up. Backup is then faster, but restoring may be slower, so if backup space is not a concern and recovery speed is, then turn off compression.
Encryption	You can have the NSA use a password to encrypt the backup files.

Table 74 Protect > Backup > Edit Job: Step 1 (continued)

LABEL	DESCRIPTION
Bandwidth	For backups to a remote NSA, you can restrict the bandwidth to help prevent the backups from using all of your network connection's available bandwidth. This is more important when backing up to a remote NSA or computer through the Internet.
Purge Policy	These fields display for archive backups. Select a policy for deleting archive backups. This purge runs first before a new backup is done. For example, if you have a backup scheduled to begin at midnight, then at that time, the NSA checks these settings and deletes files accordingly before backup takes place. If space on the backup NSA or disk is a concern, then configure the NSA to delete old backups. • **Keep All Old Backups**: Purge is in effect disabled. Select this if backup space is not a concern. • **Keep Only ___ backups**: All backup files older than the last one are deleted. You will not be able to recover files that existed (only) in those previous backups. Select this if backup space is limited and recovery of old files is not important. • **Keep Backups for ___ day(s)**: Backups older than the number of days you enter here are deleted. 0 days means that all old backups are deleted when a new one is done.
next	Click this button to proceed.

9.2.3.1 Editing a Backup Job: Step 2

Figure 172 Protect > Backup > Edit Job: Step 2



The following table describes the labels in this screen.

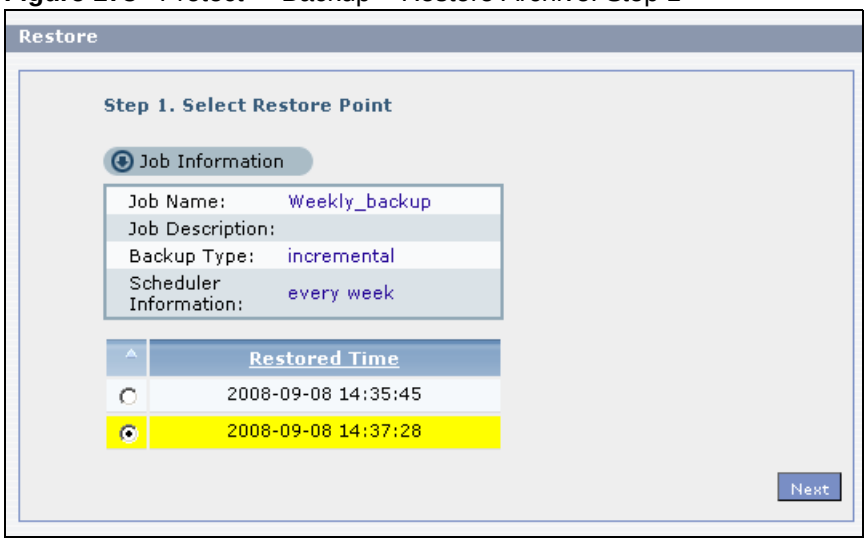
Table 75 Protect > Backup > Edit Job: Step 2

LABEL	DESCRIPTION
Backup Frequency	Select how often the job should run (**Hourly**, **Daily**, **Weekly**, or **Monthly**).
Time	Enter the time, day and/or month as appropriate for your selection above.
previous	Click this button to return to the preceding screen.
done	Click this button to save your changes back to the NSA.

9.2.4 Restoring by Backup Job

In the **Protect** > **Backup** screen, select a backup job and click the **Restore Archive** icon to replace existing files with files saved previously.

Figure 173 Protect > Backup > Restore Archive: Step 1



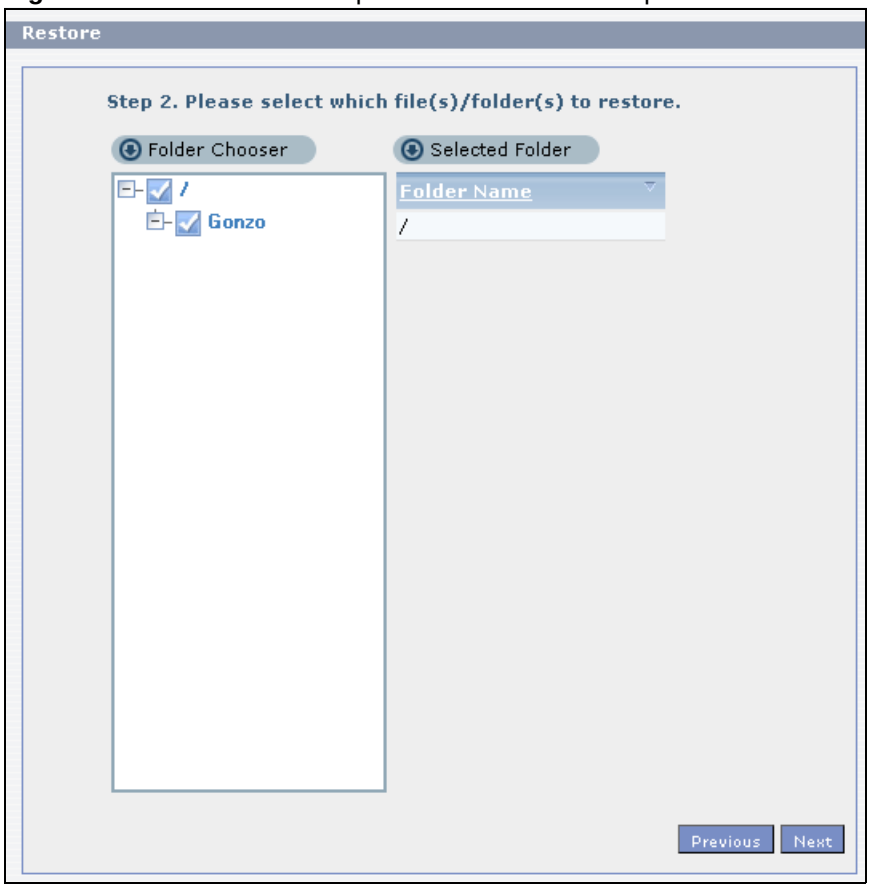
The following table describes the labels in this screen.

Table 76 Protect > Backup > Restore Archive: Step 1

LABEL	DESCRIPTION
Job Name	This is the name that identifies the backup job.
Job Description	This is some extra descriptive text on the backup.
Backup type	This displays what kind of backups the job creates.
Scheduler Information	This field displays the backup's frequency, the time it was last run in (and whether or not it succeeded), and when it is scheduled to run again. The times use yyyy-mm-dd hh:mm:ss format.
Check, Last Backup Time	Select to which backup you want to return. All later backups are deleted.
next	Click this button to proceed.

9.2.4.1 Restoring a Backup: Step 2

Figure 174 Protect > Backup > Restore Archive: Step 2



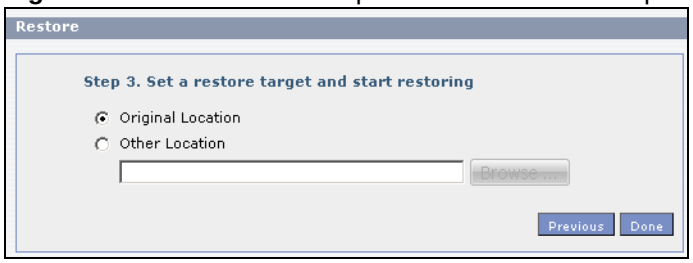
The following table describes the labels in this screen.

Table 77 Protect > Backup > Restore Archive: Step 2

LABEL	DESCRIPTION
Folder Chooser	Select the folders you want to restore.
previous	Click this button to return to the preceding screen.
next	Click this button to proceed.

9.2.4.2 Restoring a Backup: Step 3

Figure 175 Protect > Backup > Restore Archive: Step 3



The following table describes the labels in this screen.

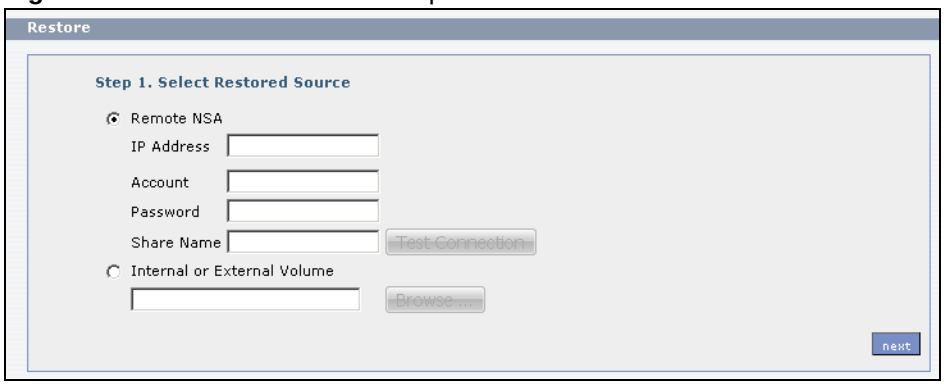
Table 78 Protect > Backup > Restore Archive: Step 3

LABEL	DESCRIPTION
Original Location	Select this option to restore the files to the place from which they were copied.
Other Location	Select this option to restore the files to somewhere other than the place from which they were copied. Type or browse for the folder to which you want to restore the backup files. Enter the backup job's password if it has one.
previous	Click this button to return to the preceding screen.
done	Click this button to save your changes back to the NSA.

9.3 Restoring by Backup Files

Click **Protect** > **Restore** to open the **Restore** screens. Use these screens to restore by the backup files if you deleted an archive backup job or the NSA or the RAID array containing the backup job failed. You can also restore a previous archive backup from another NSA or an external USB hard drive connected to the NSA.

Figure 176 Protect > Restore: Step 1



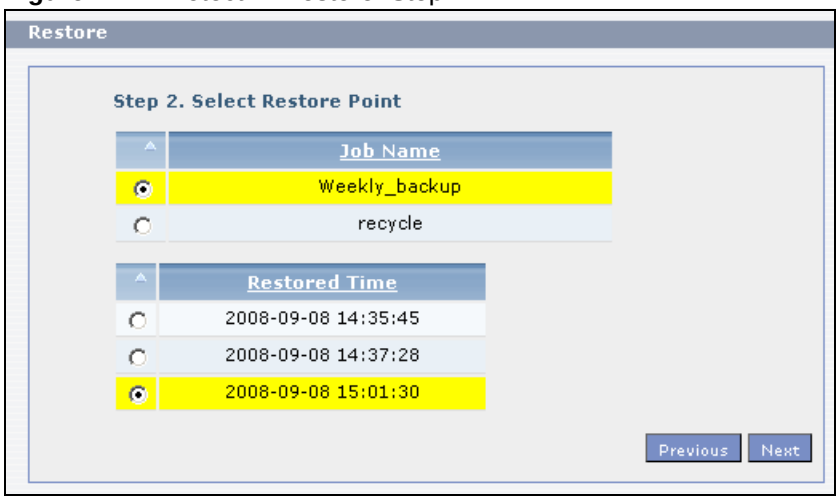
The following table describes the labels in this screen.

Table 79 Protect > Restore: Step 1

LABEL	DESCRIPTION
Remote NSA	Select this option to restore from another NSA. Type the remote NSA's IP address, user name, password, and share name.
Internal or External Volume	Select this to restore files from another volume on the NSA or a USB-connected device. Specify the share name (you can browse for it).
next	Click this button to proceed.

9.3.1 Protect > Restore: Step 2

Figure 177 Protect > Restore: Step 2



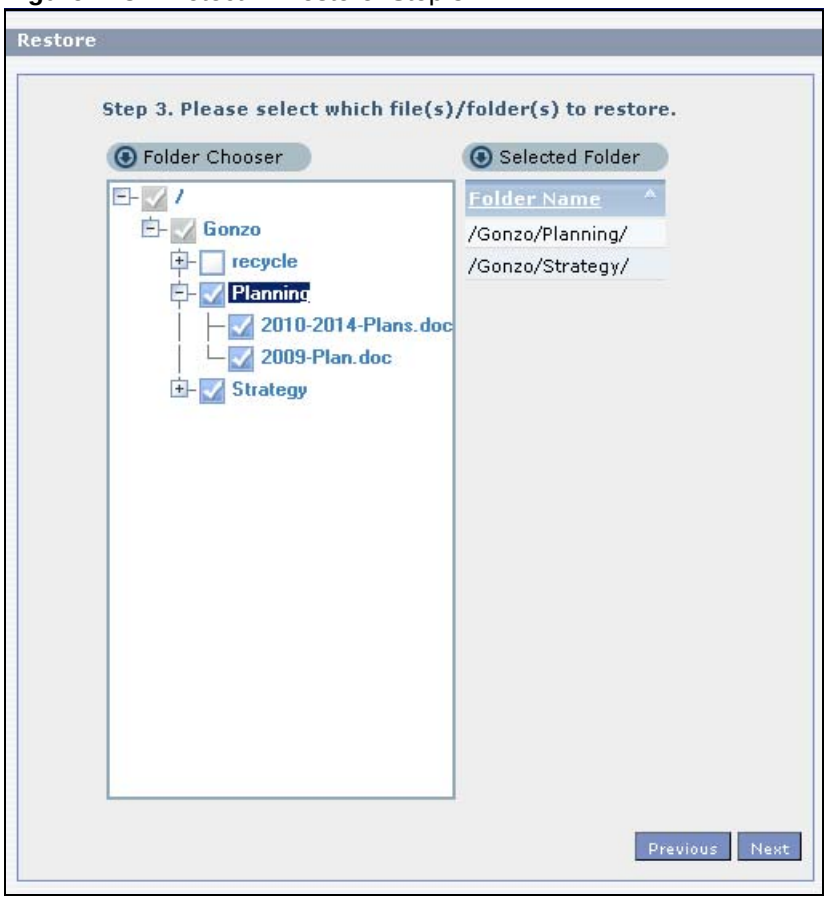
The following table describes the labels in this screen.

Table 80 Protect > Restore: Step 2

LABEL	DESCRIPTION
Select Restore Point	Select to which backup job and backup time you want to return. The NSA restores the files included in the backup archive. Files not in the backup archive are not modified.
previous	Click this button to return to the preceding screen.
next	Click this button to proceed.

9.3.2 Protect > Restore: Step 3

Figure 178 Protect > Restore: Step 3



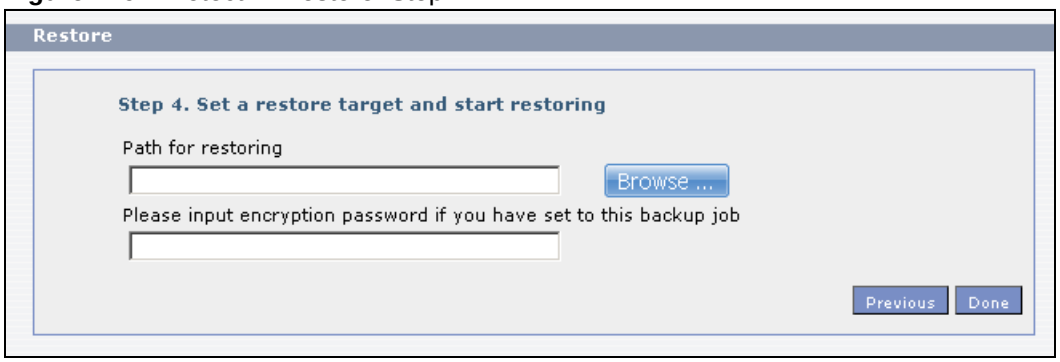
The following table describes the labels in this screen.

Table 81 Protect > Restore: Step 3

LABEL	DESCRIPTION
Folder Chooser	Select the folders you want to restore.
previous	Click this button to return to the preceding screen.
next	Click this button to proceed.

9.3.3 Protect > Restore: Step 4

Figure 179 Protect > Restore: Step 4


Restore
Step 4. Set a restore target and start restoring
Path for restoring
Browse ...
Please input encryption password if you have set to this backup job
Previous
Done

The following table describes the labels in this screen.

Table 82 Protect > Restore: Step 4

LABEL	DESCRIPTION
Path for restoring	Type or browse for the folder to which you want to restore the backup files. Enter the backup job's password if it has one.
previous	Click this button to return to the preceding screen.
done	Click this button to save your changes back to the NSA.

9.4 Snapshots

Important Notes on Snapshots

1. Snapshots can only be taken on internal volumes.
2. The NSA stores snapshots in the space on the disk array that is not used by volumes.
3. Since a snapshot is a record of changes, if very large files (typically over 1GB) are transferred onto the volume, then that 'change' may be larger than the space available for the snapshot causing it to become invalid.
4. Space available for snapshots can be decreased later by increasing the size of volumes, but not increased. (Volumes can only be made bigger, not smaller.) So it's better to leave enough unused space on a disk array when creating volumes.
5. If the disk array containing the snapshots fails, then the snapshots are lost.
6. The NSA does not take snapshots of a locked volume.

Snapshot Purging

The NSA automatically purges snapshots just before taking a new snapshot. The NSA deletes the oldest snapshot if there is no free space remaining on the disk array (space not used by volumes). If there is not enough disk space for the new snapshot, the NSA continues to delete older snapshots to make more space. It is possible that all previous snapshots will be lost.

The snapshot capture fails if deleting all previous snapshots does not leave enough space for the new snapshot. To take the snapshot, make more free space on the disk array by recreating a volume with a smaller capacity or upgrading the disk array to a larger storage capacity.

It's strongly recommended to set the maximum amount of snapshots setting as low as possible as a high amount of snapshots can significantly reduce the volume's file write performance.

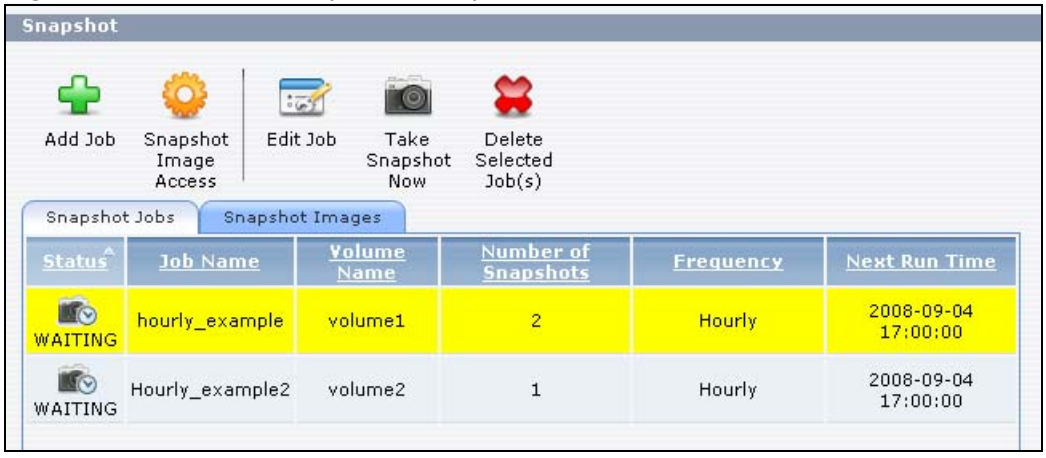
Purging of snapshots can also occur when more data is added to the volume. When more data is being written it may cause the snapshot image size to increase beyond it's original size - in this case all the snapshots on the volume will need to expand to accommodate the extra data. If there is not enough space for them all to expand, some snapshots may be deleted.

See Table 112 on page 260 for the maximum number of snapshots per volume.

A snapshot failure (dues to low disk space for example) generates a critical log. If you enable the mail log feature and set the level to critical log, the NSA sends an e-mail alert.

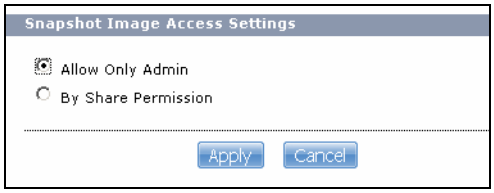
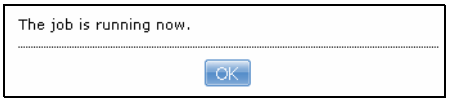
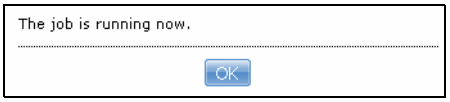
Click **Protect** > **Snapshot** in the Navigation panel to display the following screen. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 180 Protect > Snapshot > Snapshot Jobs



The following table describes the icons in this screen.

Table 83 Protect > Snapshot > Snapshot Jobs Icons

ICON	DESCRIPTION
	Add Job Click this icon to create a new snapshot job (see also Section 9.2.3 on page 208).
	Snapshot Image Access Click this icon to open a screen where you can define where the NSA stores the snapshot images (which also determines who can access them).  **Allow Only Admin**: Store all snapshots for all of a disk array's volumes in a single snapshots system share. Only the administrator can access the snapshots share by default. The administrator can change the snapshot share's share permissions. **By Share Permission**: Access each volume's snapshots in a share in the volume. Users with read access to the share can also read or copy the files in the snapshots. Each share will have a folder named snap-share for users to access the share's snapshots.
	Edit Job Select a snapshot job and click this icon to modify it's settings.
	Take Snapshot Now Select a snapshot job and click this icon to have the NSA perform the snapshot right away (instead of waiting for the scheduled time). 
	Delete Selected Job(s) Select a snapshot job(s) and click this icon to remove the job(s). 
	Sort Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

The following table describes the labels in this screen.

Table 84 Protect > Snapshot > Snapshot Jobs

LABEL	DESCRIPTION
Status	This field shows whether the snapshot job is currently running or waiting to run. The percent complete also displays for a currently running job.
Job Name	This is the name of the snapshot job.
Volume Name	This field identifies the volume upon which this job takes snapshots. A snapshot must be done on a complete volume, and not a single file or folder.
Snapshot Number	This field displays how many snapshots this job has taken so far.
Period	This field displays the snapshot schedule interval.
Next Run Time	This field displays the schedule for the next snapshot in yyyy-mm-dd hh:mm:ss format.

9.4.1 Creating/Editing Snapshots

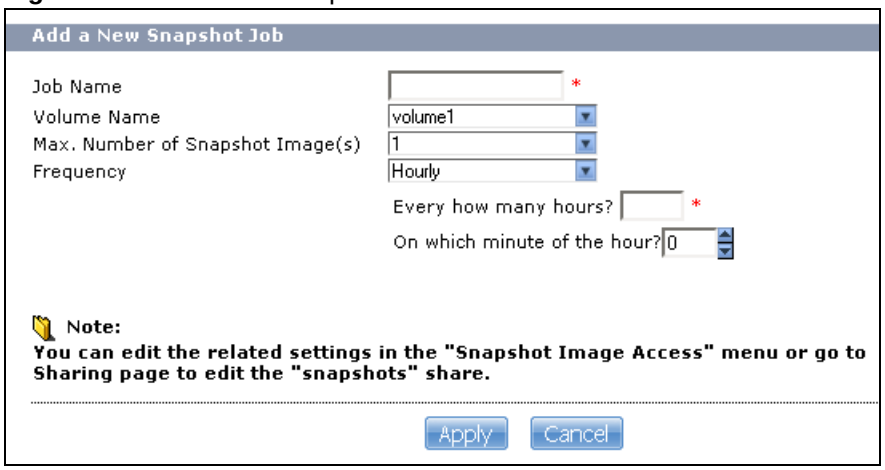
In the **Protect** > **Snapshot** screen, click the **Create Job** icon to open the following screen. Use this screen to create a new snapshot job. You can also select an existing snapshot job in the **Protect** > **Snapshot** screen and click the **Edit Job** icon.

It's strongly recommended to set the **Maximum Number of Snapshots Image(s)** as low as possible as a high amount of snapshots can significantly reduce the NSA's file write performance.

See Table 112 on page 260 for the maximum number of snapshots allowed in the NSA.

You can only create one snapshot job per volume.

Figure 181 Protect > Snapshot > Add Job



The following table describes the labels in this screen.

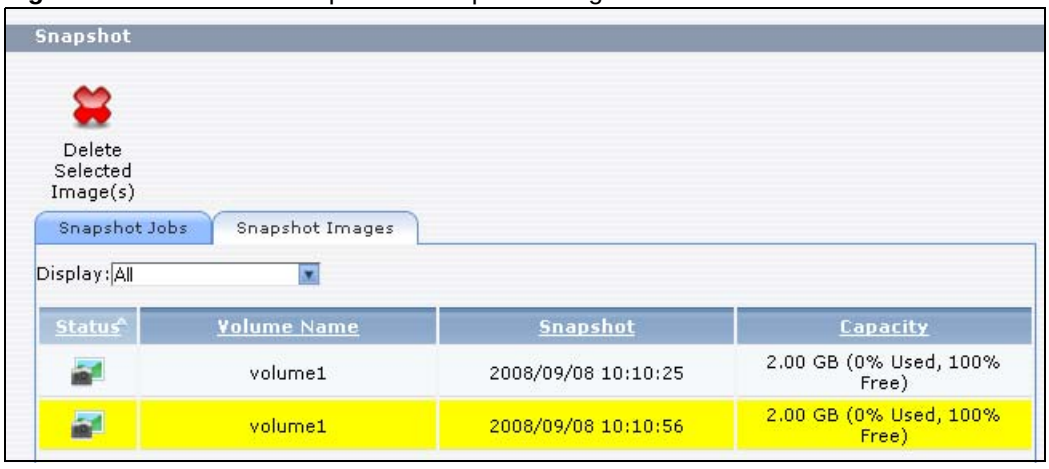
Table 85 Protect > Snapshot > Add Job

LABEL	DESCRIPTION
Job Name	This is a required field that uniquely identifies the snapshot. Type from 1 to 15 characters. You can use alphanumeric characters (A-Z 0-9) and "_" [underscores]. The first character must be a letter.
Volume Name	Select the (internal) volume to take a snapshot of. When creating a new snapshot, only volumes that are already created on the NSA are available. Note: You can only create one snapshot job per volume. A snapshot must be done on a complete volume, and not a single file or folder. However you can restore files from a snapshot on an individual file-by-file basis.
Max. Number of Snapshot Image(s)	Select the number of snapshot images to take from **1** to **5**. It's strongly recommended to set this as low as possible as each new snapshot image created will reduce the NSA's file write performance.
Period	Select how often the job should run (**Hourly**, **Daily**, or **Weekly**). It is recommended you schedule snapshots for times when your network is not busy, such as at night. If two events are configured to run at the same time, then one must wait until the other finishes running. Enter the time, and/or day as appropriate for your selection.
Apply	Click this button to save your changes back to the NSA.
Cancel	Click this button to discard your changes and exit the screen.

9.4.2 Snapshot Images

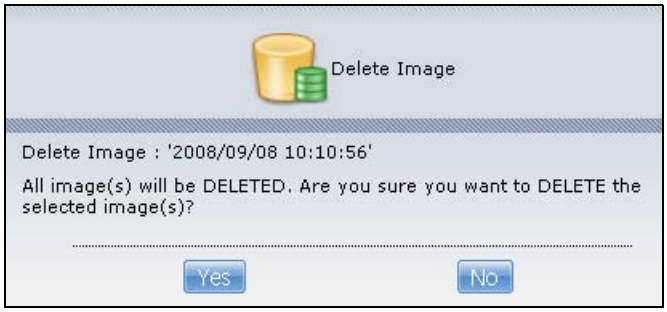
Click **Protect** > **Snapshot** > **Snapshot Images** tab to open the following screen. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 182 Protect > Snapshot > Snapshot Images



The following table describes the icons in this screen.

Table 86 Protect > Snapshot > Snapshot Images Icons

ICON	DESCRIPTION
	Delete Selected Images Select a snapshot image(s) and click this icon to remove the image(s). 
	Sort Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.
	Status This icon shows whether or not the snapshot image is valid.

The following table describes the labels in this screen.

Table 87 Protect > Snapshot > Snapshot Images

LABEL	DESCRIPTION
Display	Select for which volume you want to show snapshot images (or all).
Volume Name	This field identifies the volume that this image is a snapshot of.
Snapshot	This field displays when the snapshot image was created (in yyyy-mm-dd hh:mm:ss format).
Capacity	This field shows the storage space available for the snapshot, how much is currently in use, and how much is still available.

9.5 Backup Software Screen

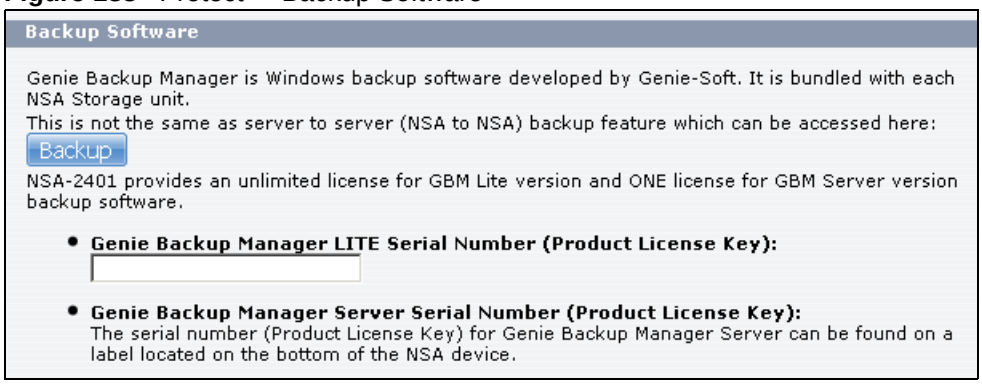
Click **Protect** > **Backup Software** to open the **Backup Software** screen.

This screen provides you with your Genie Backup Manager Lite license key and directions to find the Genie Backup Manager Server license key. You may need to use this screen if you cannot locate your license keys.

You can also locate your license keys on the back of the envelope of the CD that came with your NSA.

For more information about Genie Backup Manager please see Genie Backup Manager on page 198.

Figure 183 Protect > Backup Software


Backup Software
Genie Backup Manager is Windows backup software developed by Genie-Soft. It is bundled with each NSA Storage unit.
This is not the same as server to server (NSA to NSA) backup feature which can be accessed here:
Backup
NSA-2401 provides an unlimited license for GBM Lite version and ONE license for GBM Server version backup software.
Genie Backup Manager LITE Serial Number (Product License Key):
Genie Backup Manager Server Serial Number (Product License Key):
The serial number (Product License Key) for Genie Backup Manager Server can be found on a label located on the bottom of the NSA device.

10

Application Screens

10.1 Overview

This chapter introduces the NSA **Application** screens.

10.1.1 What You Can Do In The Application Screens

- Configure settings for FTP file transfers to/from the NSA. See Section 10.2 on page 224 for more information.
- Share a printer. See Section 10.3 on page 226 for details.
- Configure how the copy button works. See Section 10.4 on page 227 for details.

10.1.2 What You Need to Know About The Application Screens

FTP (File Transfer Protocol)

File Transfer Protocol (FTP) is a file transfer service that functions across the Internet. A system running the FTP server accepts commands from a system running an FTP client. FTP is not a secure protocol. Your file transfers could be subject to snooping.

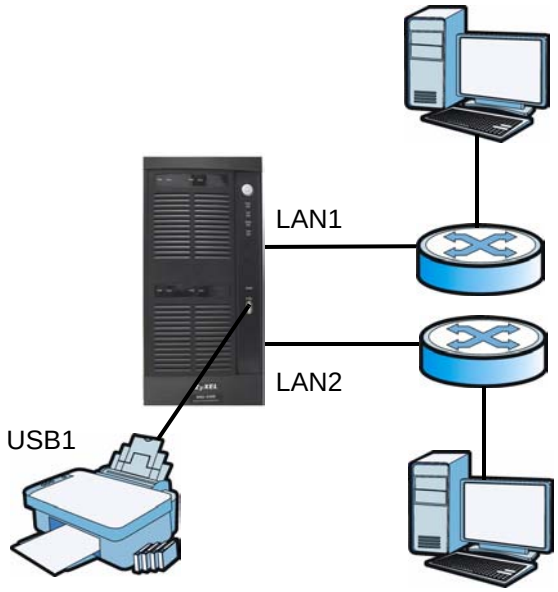
FTPES (File Transfer Protocol over Explicit TLS)

File Transfer Protocol over Explicit TLS (FTPES) is a file transfer service that uses TLS (Transport Layer Security) for secure transfers across the Internet.

Print Server

A print server is a device or software that provides users on a network with shared access to one or more printers. The print server acts as a buffer, holding the information to be printed out until the printer becomes free. The NSA can act as a print server.

Figure 184 Printer Sharing

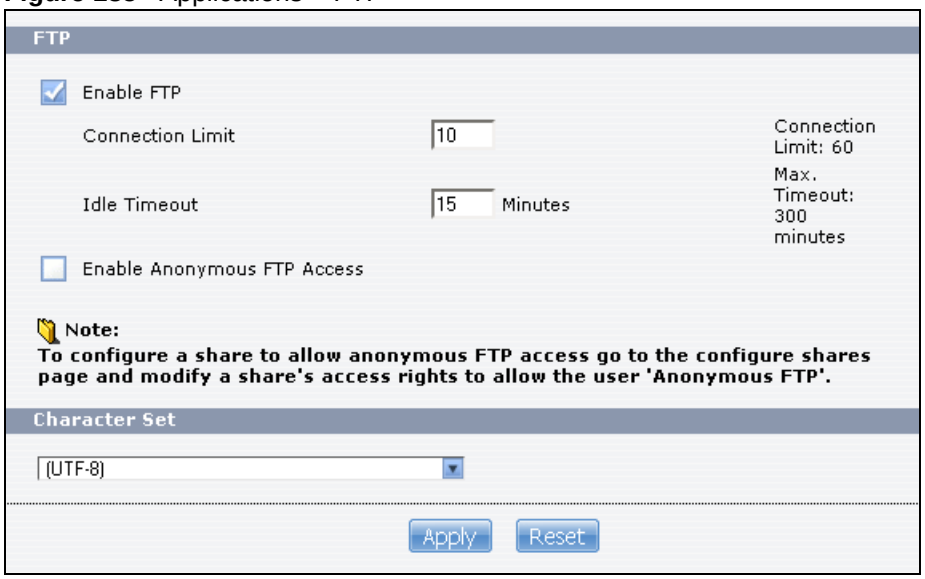


10.2 FTP

Click **Applications** > **FTP** to open this screen and configure settings for transferring files to and from the NSA using FTP (File Transfer Protocol) or FTP over Explicit TLS.

Your FTP client must be set to use FTP over Explicit TLS in order to use FTPES with the NSA.

Figure 185 Applications > FTP



The following table describes the labels in this screen.

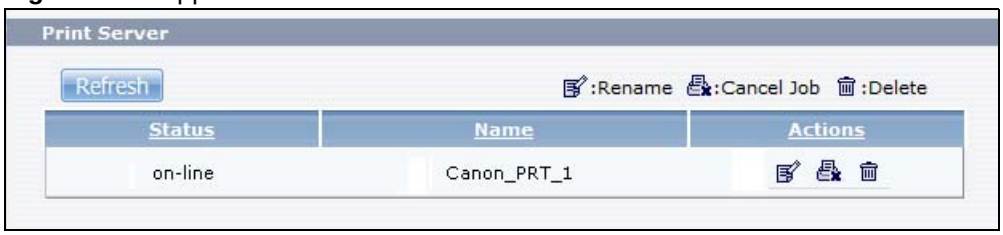
Table 88 Applications > FTP

LABEL	DESCRIPTION
Enable FTP	Select this to allow users to connect to the NSA via FTP. This also enables FTP over Explicit TLS (FTPES). You can use FTP or FTPES to send files to the NSA or get files from the NSA.
Connection Limit	Enter the maximum number of concurrent FTP connections allowed on the NSA in this field.
Idle Timeout	Enter the length of time that an FTP connection can be idle before being disconnected by the NSA.
Enable Anonymous FTP Access	Select this to allow any user to log into the NSA using ‘FTP’ or ‘anonymous’ as a username and no password. Any other name is considered a username, so must be valid and have a corresponding correct password.
Character Set	Select the appropriate language encoding here If the NSA’s folders or file names do not display correctly in your FTP client. The NSA uses UTF-8 format for FTP by default. This setting applies to all FTP client connections to the NSA. It does not affect your Windows/CIFS connections (it will not correct the character display in Windows Explorer).
Apply	Click this to save your changes.
Reset	Click this to discard any changes and start again.

10.3 Print Server

Click **Applications** > **Print Server** to open this screen. Use this screen to view and manage the NSA's list of printers and print jobs.

Figure 186 Applications > Print Server



The following table describes the labels in this screen.

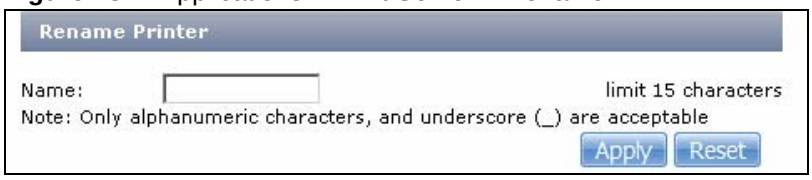
Table 89 Applications > Print Server

LABEL	DESCRIPTION
Refresh	Click this to update the list of printers and print jobs.
Status	This fields shows whether the printer is connected and turned on (**on-line**) or not (**off-line**).
Name	This identifies the printer. Each printer connected to the NSA must use a unique name.
Actions	**Rename** Click this to change the name the NSA uses for the printer. **Cancel Job** Click this to remove all print jobs from the NSA queue for a particular printer. However, since the NSA sends print jobs to the printer as soon as it can, this button may only have an effect if there are very large or many print jobs in the queue. To stop a print job that has already started, you may have to turn off the printer. **Delete** Click this to remove a printer from the NSA's printer list. To add the printer back into the list, disconnect the printer from the NSA's USB port and reconnect it. If that does not work, disconnect the USB port and turn off the printer's power. Then reconnect the printer and turn it back on.

10.3.1 Print Server Rename

Click **Applications** > **Print Server**, select a printer from the list, and then click that printer's **Rename** icon to open this screen. Use this screen to change the name that the NSA uses for the printer.

Figure 187 Applications > Print Server > Rename



The following table describes the labels in this screen.

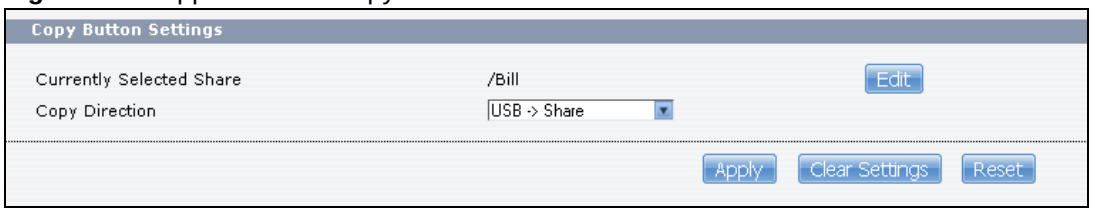
Table 90 Applications > Print Server > Rename

LABEL	DESCRIPTION
Name	Type a new name to identify the printer. The name must be unique from all the other names of printers connected to the NSA.
Apply	Click this to save your changes.
Reset	Click this to discard any changes and start again.

10.4 Copy Button

Click **Applications** > **Copy Button** to open this screen. Use the **COPY** button on the front panel of the NSA to copy files between a USB flash drive or externally connected hard disk and a share in the NSA. If more than one USB device is connected to the NSA, the NSA uses the USB device that was most recently connected.

Figure 188 Applications > Copy Button



The following table describes the labels in this screen.

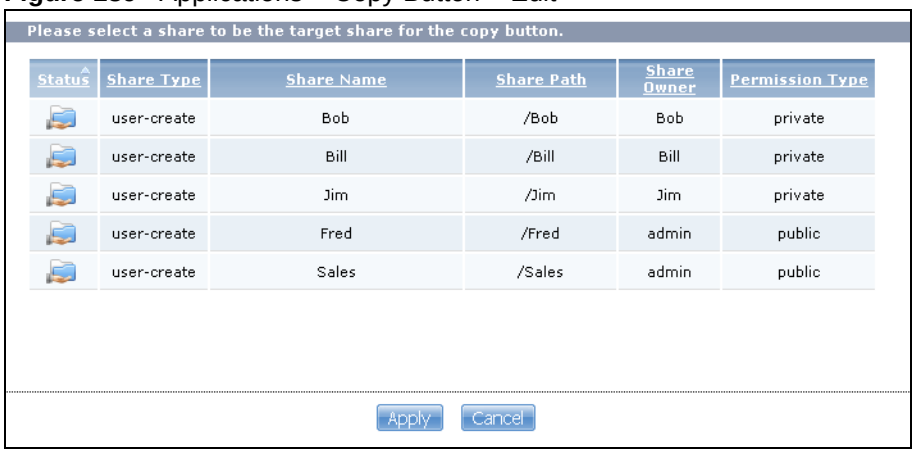
Table 91 Applications > Copy Button

LABEL	DESCRIPTION
Currently Selected Share	This field displays the share that the NSA is set to use with the copy button feature.
Edit	Click this button to use a different share with the copy button feature.
Copy Direction	Select whether you want to use the copy button to copy files from the USB device to the share on the NSA or from the share on the NSA to the USB device.
Apply	Select a share, then click this to make it the default location where data is stored when you press the copy button.
Clear Settings	Click this to reset this screen to the default settings.
Reset	Click this to discard any changes and start again.

10.4.1 Changing the Copy Button Share

Click **Applications** > **Copy Button** and then **Edit** to open the following screen. Use this screen to select the share the NSA uses with the copy button.

Figure 189 Applications > Copy Button > Edit



The following table describes the icons in this screen.

Table 92 Applications > Copy Button > Edit

ICON	DESCRIPTION
	Available Share Indicates the share can be used for file and folder management.
	Unavailable Share Indicates the share cannot be used because the NSA cannot find the physical location of the share.
	Disabled Share Indicates the share is no longer functional. If this happens, talk to your network administrator.

The following table describes the labels in this screen.

Table 93 Applications > Copy Button > Edit

LABEL	DESCRIPTION
Status	This column displays whether the share is **Available**, **Unavailable** or **Disabled**.
Share Type	This displays whether the share is created by the system or by the administrator.
Share Name	This displays the name of the share on the NSA.
Share Path	This displays the location of the shared folder on the NSA. Forward slashes are used as path (folder tree branch) separators. Share paths that no longer exist are shown in red.
Share Owner	This displays the name of the user account that owns the share.
Permission Type	This displays the type of permissions assigned to the share. Options are public, private, and advanced.
Apply	Select a share, then click this to make it the default location where data is stored when you press the copy button.
Reset	Click this to discard any changes and start again.

11

Maintenance Screens

11.1 Overview

This chapter introduces the NSA **Maintenance** screens.

11.1.1 What You Can Do In The Maintenance Screens

- View the NSA system logs. See Section 11.2 on page 230 for details.
- Manage the NSA configuration file. See Section 11.3 on page 237 for details.
- Configure HTTPS and the NSA's SSL certificate. See Section 11.4 on page 239 for details.
- Upload new firmware. See Section 11.5 on page 241 for details.
- Set the power management settings. See Section 11.6 on page 242 for details.
- Restart or turn off your NSA. See Section 11.7 on page 245 for details.

11.1.2 What You Need to Know About The Maintenance Screens

HTTPS

HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

Public Key Certificate

Public key certificates are used by web browsers to ensure that a secure web site is legitimate. When a certificate authority such as VeriSign, Comodo, or Network Solutions, to name a few, receives a certificate request from a website operator, they confirm that the web domain and contact information in the request match those on public record with a domain name registrar. If they match, then the certificate is issued to the website operator, who then places it on his site to be issued to all visiting web browsers to let them know that the site is legitimate.

Syslog Server

The syslog protocol is built around data logging for the purposes of keeping records and analysis. On a typical network the syslog daemon can be configured to send system logs to a central online repository known as a syslog server. This allows the network administrators to quickly access and examine them without having to go to every machine on the network.

Finding Out More

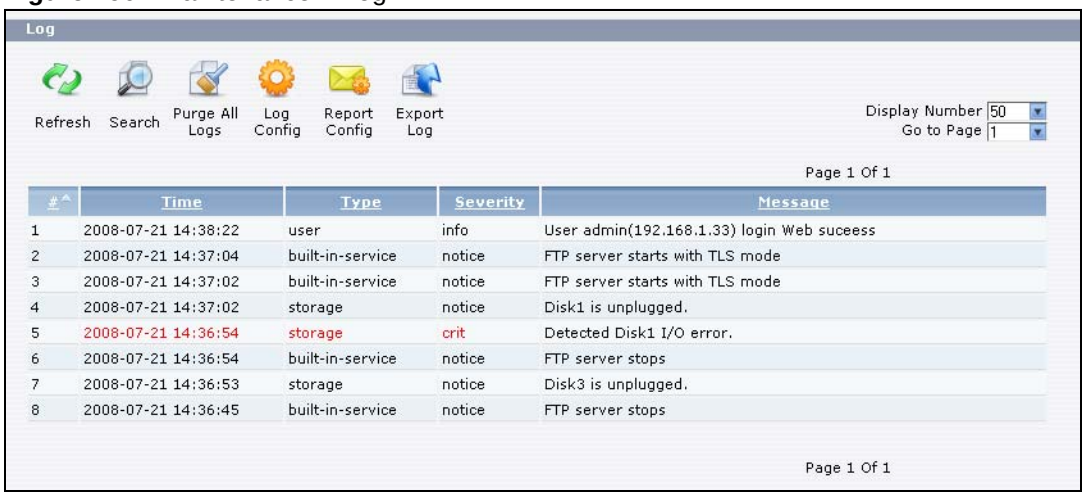
See Section 3.5 on page 68 for tutorials on configuring security.

See Section 3.6 on page 89 for a tutorial on power resume.

11.2 Log

Click **Maintenance** > **Log** to open a screen that displays all NSA activity logs.

Figure 190 Maintenance > Log


Log
Refresh
Search
Purge All Logs
Log Config
Report Config
Export Log
Display Number 50
Go to Page 1
Page 1 Of 1
Time Type Severity Message
1 2008-07-21 14:38:22 user info User admin(192.168.1.33) login Web suceess
2 2008-07-21 14:37:04 built-in-service notice FTP server starts with TLS mode
3 2008-07-21 14:37:02 built-in-service notice FTP server starts with TLS mode
4 2008-07-21 14:37:02 storage notice Disk1 is unplugged.
5 2008-07-21 14:36:54 storage crit Detected Disk1 I/O error.
6 2008-07-21 14:36:54 built-in-service notice FTP server stops
7 2008-07-21 14:36:53 storage notice Disk3 is unplugged.
8 2008-07-21 14:36:45 built-in-service notice FTP server stops
Page 1 Of 1

The following table describes the icons in this screen.

Table 94 Maintenance > Log Icons

ICON	DESCRIPTION
	Refresh Click this icon to update the log display.
	Search Click this icon to display the search filters which you can use to search for specific text and/or criteria in the log collection. See Section 11.2.1 on page 232 for more information.
	Purge All Logs Click this icon to erase all logs from the NSA. Click **Yes** to remove all logs or **No** to cancel.

Table 94 Maintenance > Log Icons (continued)

ICON	DESCRIPTION
	Log Config Click this icon to open **Log Configuration** screen. See Section 11.2.2 on page 232 for more information.
	Report Config Click this icon to open the **Log Report Configuration** screen, where you can set up how logs are handled. See Section 11.2.4 on page 233 for details.
	Export Log Click this button to export the selected log(s).

The following table describes the labels in this screen.

Figure 191 Maintenance > Log

LABEL	DESCRIPTION
#	This is the log entry's number in the list according to the currently selected sort order.
Time	This shows the date and time the log was created. Click the top of the column to sort by oldest or newest.
Type	This displays the log category.
Severity	This displays how serious the log is rated by the NSA. The severity ratings are: **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, and **Info**.
Message	This displays a description of the log. Click the top of the column to sort by alphabetical or reverse alphabetical order.
Display Number	Set the number of logs displayed per page.
Go to Page	Select a page number of logs to display.
Previous & Next	Click **Previous** to cycle back through the pages of logs, and **Next** to cycle forward through them. If only one page exists, then clicking either of these simply refreshes the page.

11.2.0.1 Log Classes

The NSA keeps detailed records of all activity that occurs on it. These records, or logs, are organized according to "class". The following table describes the different log classes.

Figure 192 Maintenance > Log > Log Classes

LOG	CLASS DESCRIPTION
Action-log	If you enable the action log feature for a share(s), this class shows information about when users upload or download files or folders or create folders.
User	This class shows information on user account access to the NSA.
Share	This class shows information on shares being created or deleted.
Service	This class shows information on the operation of the NSA's built-in services.
System	This class shows all other system related messages.
Network	This class shows information on network configuration, setting changes and so on.
Storage	This class shows information about the NSA's internal and external storage activity.

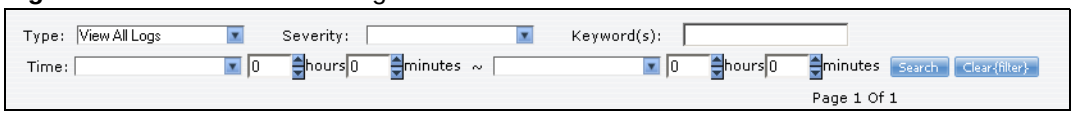
Figure 192 Maintenance > Log > Log Classes (continued)

LOG	CLASS DESCRIPTION
Application	This class shows information about the NSA's FTP, print server, and copy button applications.
Backup	This log class shows information about all backup-related activity.

11.2.1 Search

Click the **Maintenance** > **Log** > **Search** icon to display the search filters.

Figure 193 Maintenance > Log > Search Filters



The following table describes the labels in this screen.

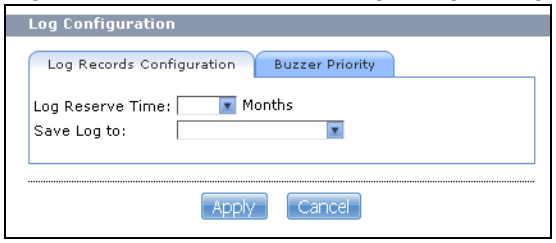
Table 95 Maintenance > Log > Search Filters

LABEL	DESCRIPTION
Type	This filters search results according to the log type selected. The default setting is **View All Logs**.
Severity	This filters search results according to the severity rating selected. When you select a severity, the NSA searches through all logs of that severity or higher. The default is to search through all files regardless of severity.
Keyword(s)	Enter a specific word for which to search. The default is all words.
Time	This filters search results according to the time frame selected in the beginning date and end date fields. The default is any time frame since the first existing log file was generated. (Purged logs, of course, cannot be searched.) To set a start date, click the left menu and pick a day from the calendar. To set an end date, click the right menu and pick a day from the calendar.
Search	Click to begin searching according to the search parameters you set. If you choose not to set any search parameters, then the defaults for each filter is used.
Clear {filter}	Click to reset all the search filters back to their default settings.

11.2.2 Log Records Configuration

Click **Maintenance** > **Log** > **Log Config** to open the **Log Records Configuration** screen, where you can customize the duration that logs are kept on the NSA.

Figure 194 Maintenance > Log > Log Config > Log Records Configuration



The following table describes the labels in this screen.

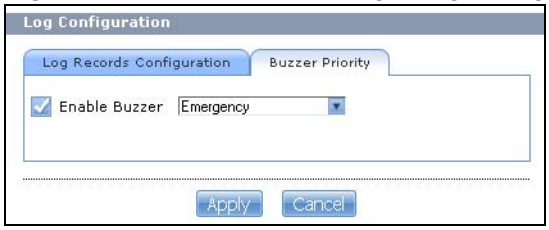
Table 96 Maintenance > Log > Log Config > Log Records Configuration

LABEL	DESCRIPTION
Log Reserve Time:	Set the number of months, up to 10, to keep the logs stored on the NSA.
Save Log to:	Select a user account on whose share you want to store the logs. The system default stores logs in a neutral location.
Apply	Click this to save your changes.
Cancel	Click this to discard changes and close the window.

11.2.3 Log Buzzer Priority Configuration

Click **Maintenance** > **Log** > **Log Config** > **Buzzer Priority** to open a screen where you can configure the audible buzzer's settings. enable or disable the audible buzzer alarm feature and set what severity level of logs trigger it.

Figure 195 Maintenance > Log > Log Config > Buzzer Priority



The following table describes the labels in this screen.

Table 97 Maintenance > Log > Log Config > Buzzer Priority

LABEL	DESCRIPTION
Enable Buzzer	Select this option to enable the audible buzzer alarm feature. Use the drop-down list box to select the severity level of log that triggers the audible buzzer. When you enable this feature, the NSA sounds an audible alarm buzzer if it generates a log of a severity level equal to or higher than the one selected in the drop-down list box to the right.
Apply	Click this to save your changes.
Cancel	Click this to discard changes and close the window.

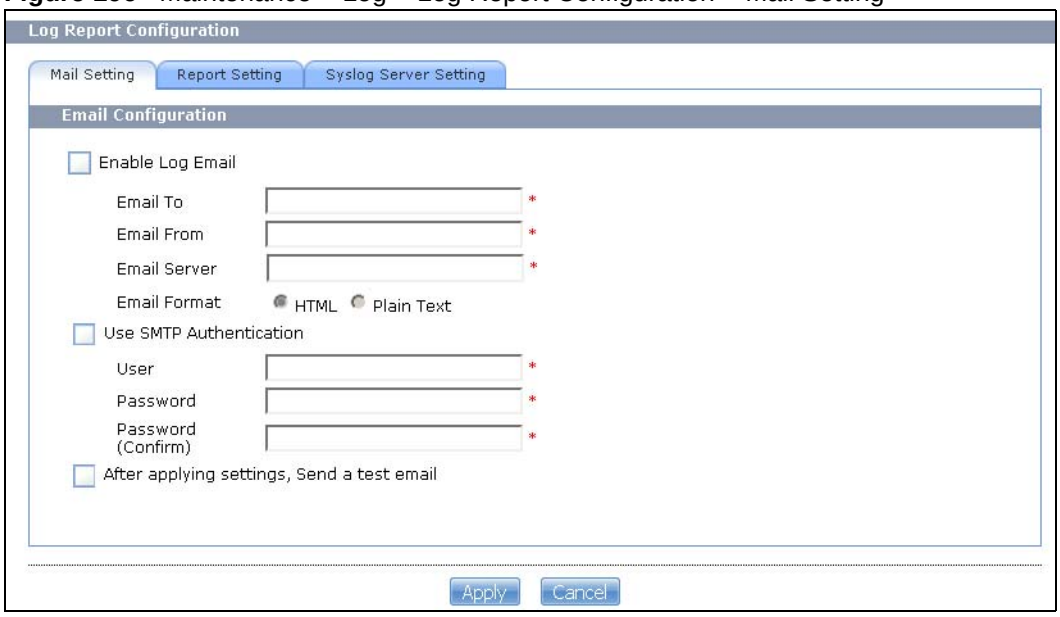
11.2.4 Report Configuration

Click **Maintenance** > **Logs** > **Report Config** to open the report configuration screens.

11.2.4.1 Mail Setting

This screen lets you configure whether or not logs are e-mailed.

Figure 196 Maintenance > Log > Log Report Configuration > Mail Setting



The following table describes the labels in this screen.

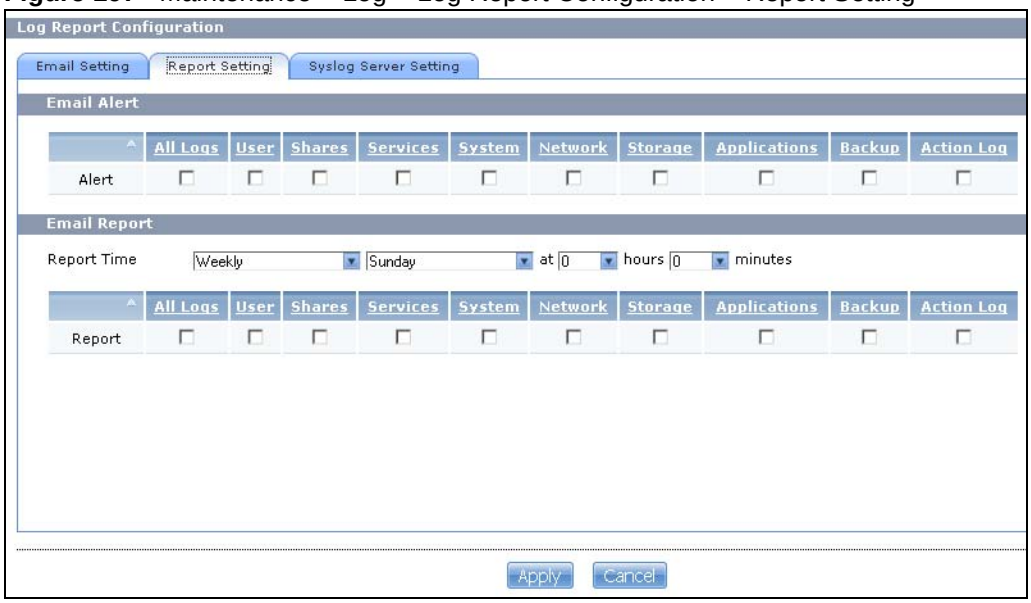
Table 98 Maintenance > Log > Log Report Configuration > Mail Setting

LABEL	DESCRIPTION
Enable Log Email	Select this option to have the NSA periodically send log files by e-mail to the account specified in the options below.
Email To	Enter the e-mail address to which you want the logs e-mailed.
Email From	Enter the e-mail address from which you want the logs e-mailed. This is the address that appears in the e-mail's **From:** field.
Email Server	Enter the SMTP server the NSA will use to send the e-mail.
Email Format	Select whether to send e-mails as HTML or as plain text.
Use SMTP Authentication	Check this option if your SMTP mail server requires authentication in order to send e-mails. If so, then you must also fill in the **Account** and **Password** fields.
User	Enter the account name with which you log into your SMTP mail server.
Password	Enter the password for the account name with which you log into your SMTP mail server.
Password (Confirm)	Re-enter the password for the account name with which you log into your SMTP mail server to ensure you have entered it correctly.
After applying settings, Send a test email	Select this to have the NSA send an e-mail so you can may sure the settings are correct and the NSA's sending of e-mail is working properly.
Apply	Click this to save your changes.
Cancel	Click this to discard changes and close the window.

11.2.4.2 Report Setting

This screen lets you configure which types of logs are e-mailed during alerts and reports.

Figure 197 Maintenance > Log > Log Report Configuration > Report Setting



The following table describes the labels in this screen.

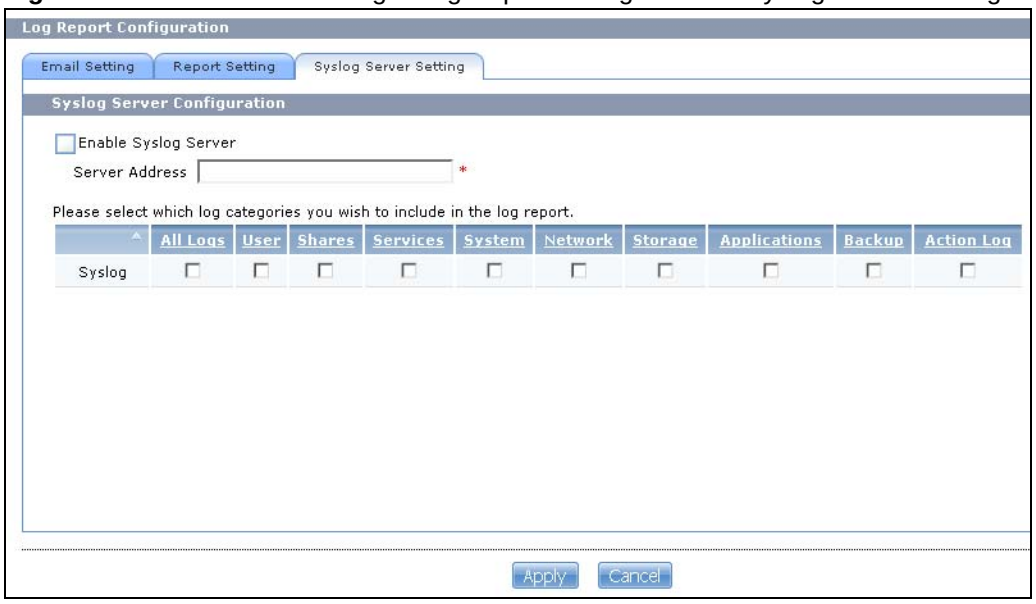
Table 99 Maintenance > Log > Log Report Configuration > Report Setting

LABEL	DESCRIPTION
Alert	Select the kind of log(s) to be sent out during mail alerts. Alerts are issued when a critical or system event requires immediate attention. See Section 11.2.0.1 on page 231 for information on the different log classes.
Report Time	Set the frequency with which log files are mailed out.
Report	Select the kind of log(s) to be sent out during mail reports. Reports are issued at set intervals. See Section 11.2.0.1 on page 231 for information on the different log classes.
Apply	Click this to save your changes.
Cancel	Click this to discard changes and close the window.

11.2.4.3 Syslog Server Setting

This screen lets you set up the NSA to upload log files to a syslog server.

Figure 198 Maintenance > Log > Log Report Configuration > Syslog Server Setting



The following table describes the labels in this screen.

Table 100 Maintenance > Log > Log Report Configuration > Syslog Server Setting

LABEL	DESCRIPTION
Enable Syslog Server	Select this option to have the NSA upload its log files to the syslog server.
Server Address	Enter the syslog server's IP address in this field when the **Enable Syslog Server** option is selected.
Syslog	Choose the type of logs to upload to the syslog server. See Section 11.2.0.1 on page 231 for information on the different log classes.
Apply	Click this to save your changes.
Cancel	Click this to discard changes and close the window.

11.2.5 Export Log

Click **Maintenance** > **Log** and then select a log from the list. To export it, click the **Export Log** icon. Your web browser prompts you to download the log file as a CSV (Comma Separated Value) file type, which is compatible with Microsoft Excel and other spreadsheet software.

11.3 Configuration

Click **Maintenance** > **Configuration** to open a screen where you can backup and restore the NSA configuration settings or restore the device to its factory default settings.

Figure 199 Maintenance > Configuration

Backup Current Configuration Settings
Click the Backup button to save the current configuration of our system to your local computer.
Include Volume Encryption Settings
Backup
Restore Configuration
To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Restore.
Step1 Restore File:
Browse...
Upload
Step2 Select Restore Type:
Restore Configuration
Restore Volume Encryption Settings
Restore
Reset to Default
Reset to Default
This action will reset all your setting to default values and reboot NSA-2401.

The following table describes the labels in this screen.

Table 101 Maintenance > Configuration

LABEL	DESCRIPTION
Backup Current Configuration Settings	
Include Volume Encryption Settings	Select this to have the configuration file include settings for unlocking the encrypted volumes (either by manually entering a password or using a USB key). The password itself is not saved in the configuration file.
Backup	Click this button to save the current NSA configuration to your computer. Your browser prompts you to save the file.
Restore Configuration	
Browse	Click this button to locate a previously-saved configuration file on your computer or network location.
Upload	Click this button to load the previously-saved configuration file to the NSA. This does not automatically apply the configuration file's settings.
Restore Configuration	After you upload a configuration file to the NSA, select this to replace the NSA's general configuration settings with the settings in the file you uploaded. This does not include the volume encryption settings.
Restore Volume Encryption Settings	This option is available if you included the volume encryption settings when you backed up the configuration. Select this and an encrypted volume(s) to restore the settings for unlocking the encrypted volume(s). This restores the unlocking settings to what they were when you created the backup. So whatever the encrypted volume's password or USB key was when you created the backup, use the same to unlock the encrypted volume.
Restore	Click this to replace the selected NSA configuration settings with those in the file you uploaded.

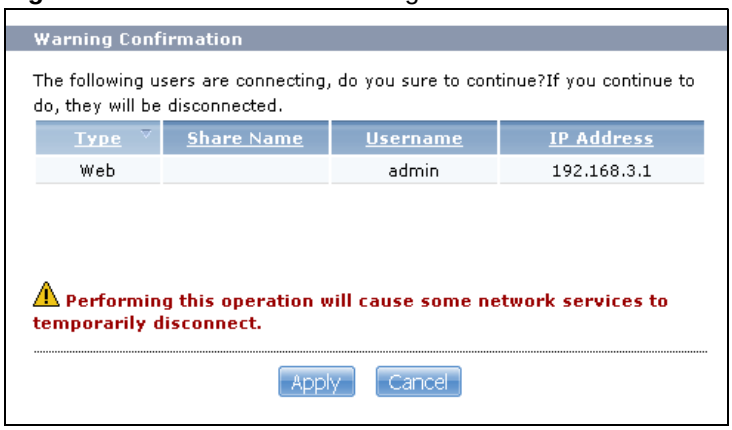
Table 101 Maintenance > Configuration

LABEL	DESCRIPTION
Reset to Default	
Reset to Default	Click this to restore the NSA to its factory default settings.

11.3.1 Restoring the Configuration File

When restoring a previously saved configuration file, you are presented with a warning screen if any users are connected.

Figure 200 Maintenance > Configuration > Restore



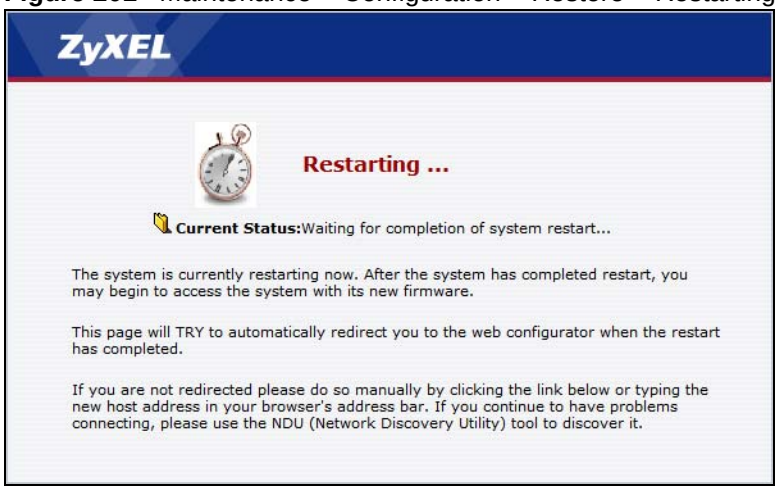
The following table describes the labels in this screen.

Table 102 Maintenance > Configuration

LABEL	DESCRIPTION
Type	Indicates the kind of connection the user has to the NSA.
Share Name	Indicates the share to which the user is currently connected.
Username	Indicates the user account name.
IP Address	Indicates the user's originating IP address.
Apply	Click this to save your changes.
Cancel	Click this to discard changes and close the window.

If the NSA is free of all connections, then configuration file loads and the NSA restarts itself.

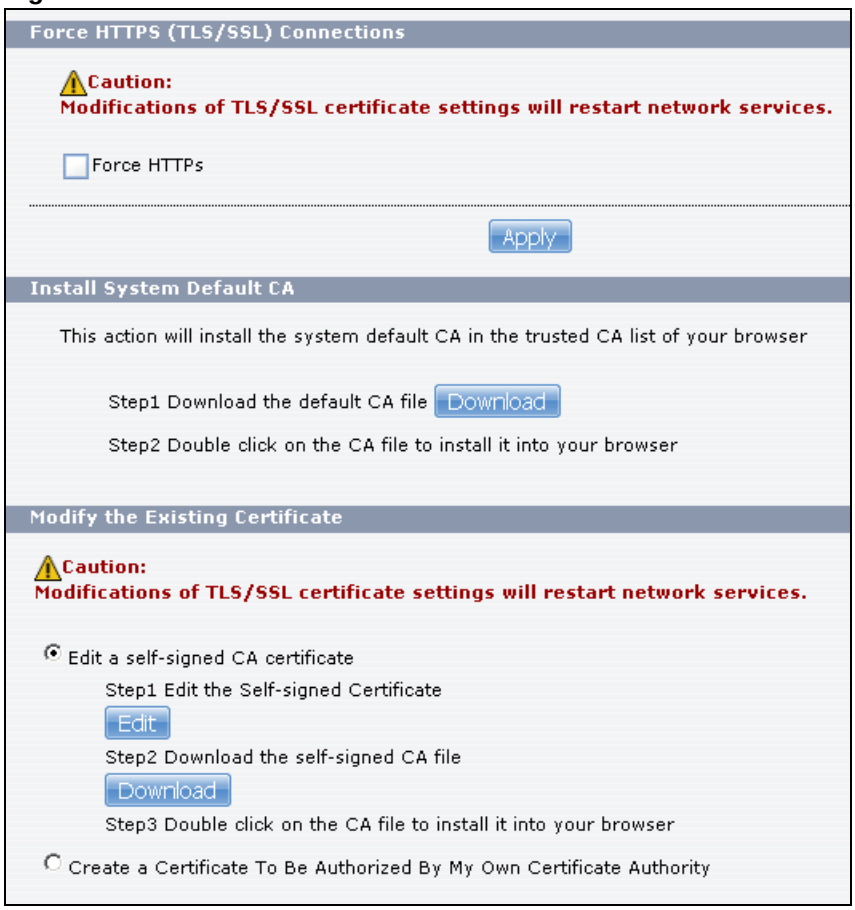
Figure 201 Maintenance > Configuration > Restore > Restarting


ZyXEL
Restarting ...
Current Status:Waiting for completion of system restart...
The system is currently restarting now. After the system has completed restart, you may begin to access the system with its new firmware.
This page will TRY to automatically redirect you to the web configurator when the restart has completed.
If you are not redirected please do so manually by clicking the link below or typing the new host address in your browser's address bar. If you continue to have problems connecting, please use the NDU (Network Discovery Utility) tool to discover it.

11.4 SSL

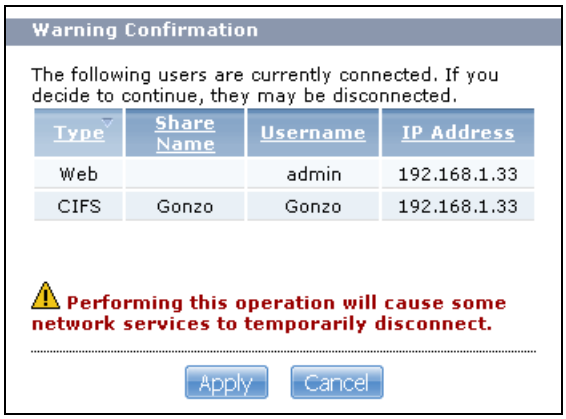
Click **Maintenance** > **SSL** to open this screen, where you can turn on HTTPS, create a public key certificate, or upload a public key certificate that was issued by a known certificate authority.

Figure 202 Maintenance > SSL


Force HTTPS (TLS/SSL) Connections
Caution:
Modifications of TLS/SSL certificate settings will restart network services.
Force HTTPs
Apply
Install System Default CA
This action will install the system default CA in the trusted CA list of your browser
Step1 Download the default CA file
Download
Step2 Double click on the CA file to install it into your browser
Modify the Existing Certificate
Caution:
Modifications of TLS/SSL certificate settings will restart network services.
Edit a self-signed CA certificate
Step1 Edit the Self-signed Certificate
Edit
Step2 Download the self-signed CA file
Download
Step3 Double click on the CA file to install it into your browser
Create a Certificate To Be Authorized By My Own Certificate Authority

The following table describes the labels in this screen.

Table 103 Maintenance > SSL

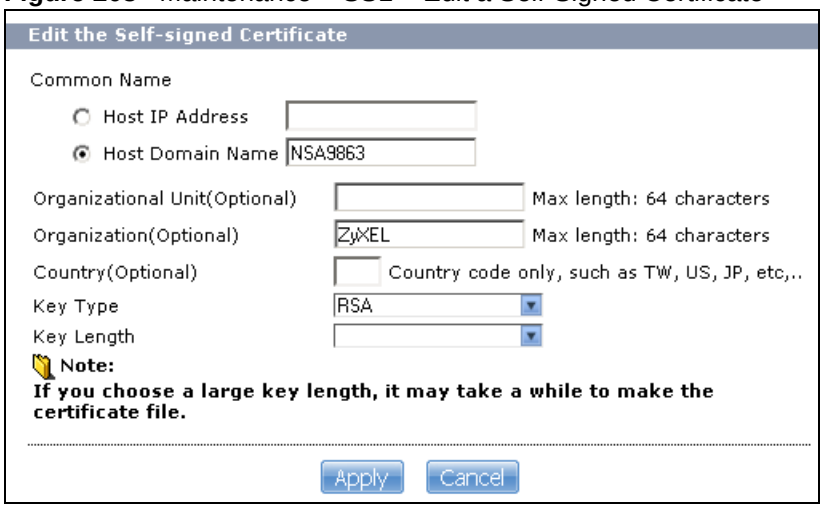
LABEL	DESCRIPTION
Force HTTPs	Select the **Force HTTPs** option to turn on the NSA's web browser security. Anyone who connects via HTTPS to the NSA must install the public key certificate associated with it. The NSA displays a warning screen if applying your change may disconnect some users. Click **Apply** if you want to continue. 
Install System Default CA	Click **Download** button to save a copy of the NSA's public key certificate to your local computer. This is useful for installing the certificate without having to connect to the NSA, or for sending by email to other users for them to install prior to logging into the NSA for the first time. After saving the certificate to your computer, double-click it to install it. Note: Each web browser handles certificate installation differently. See Appendix C on page 299 for more information.
Modify the Existing Certificate	Select **Edit a self-signed CA certificate**, then follow the on-screen instructions for creating a public key certificate signed by the NSA as the local certificate authority. Note: Use certificates created and signed by the NSA if the device is not open to external access. Select **Create a certificate authorized by other CA**, then follow the on-screen instructions to install a certificate that has been authorized by a third-party certificate authority. Note: Use this method if the device is open to external access, such as allowing users to connect through the Internet using FTP over Explicit TLS or HTTPs.

11.4.0.1 Editing a Self-Signed Certificate or Creating a Certificate Signing Request

When you select the **Edit a self-signed CA certificate** option, then click the **Edit** button, a screen opens to allow you to make adjustments to the NSA's public key certificate.

The screen is also the same for the **Create a certificate authorized by other CA** option.

Figure 203 Maintenance > SSL > Edit a Self-Signed Certificate



The following table describes the labels in this screen.

Table 104 Maintenance > Configuration

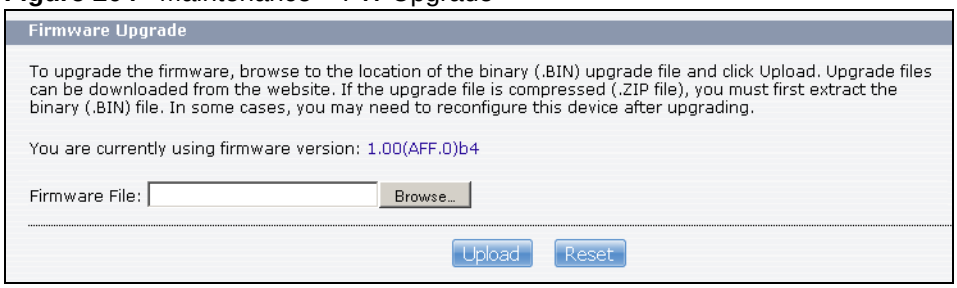
LABEL	DESCRIPTION
Common Name	This name describes the certificate's origin, either in the form of an IP address or a domain name.
Host IP Address	Select this option and enter the NSA's IP address if you want to use this for the common name.
Host Domain Name	Select this option and enter the NSA's domain name if you want to use this for the common name
Organizational Unit (Optional)	Enter this name of the organizational unit which owns or maintains the NSA. This is an optional field.
Organization (Optional)	Enter this name of the organization or company which owns or maintains the NSA. This is an optional field.
Country (Optional)	Enter this name of the country in which the NSA is located. This is an optional field.
Key Type	Select the certificate's key type, either **RSA** or **DSA**.RSA is a public-key encryption and digital signature algorithm, while DSA is only a digital signature algorithm.
Key Length	Select the encryption key length. The longer the key, the better the encryption security. The only drawback to having a long key is that the file encrypted with it swells in size as well.
Apply	Click this to save your changes.
Cancel	Click this to discard changes and close the window.

11.5 Firmware Upgrade

Click **Maintenance** > **FW Upgrade** to open this screen, where you can upgrade the NSA firmware. Be sure to download the latest firmware files from the ZyXEL website.

The **SYS** LED blinks orange when firmware is being uploaded to the NSA. Do not turn off or reset the NSA while the firmware update is in progress!

Figure 204 Maintenance > FW Upgrade


Firmware Upgrade
To upgrade the firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from the website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure this device after upgrading.
You are currently using firmware version: 1.00(AFF.0)b4
Firmware File:
Browse...
Upload
Reset

The following table describes the labels in this screen.

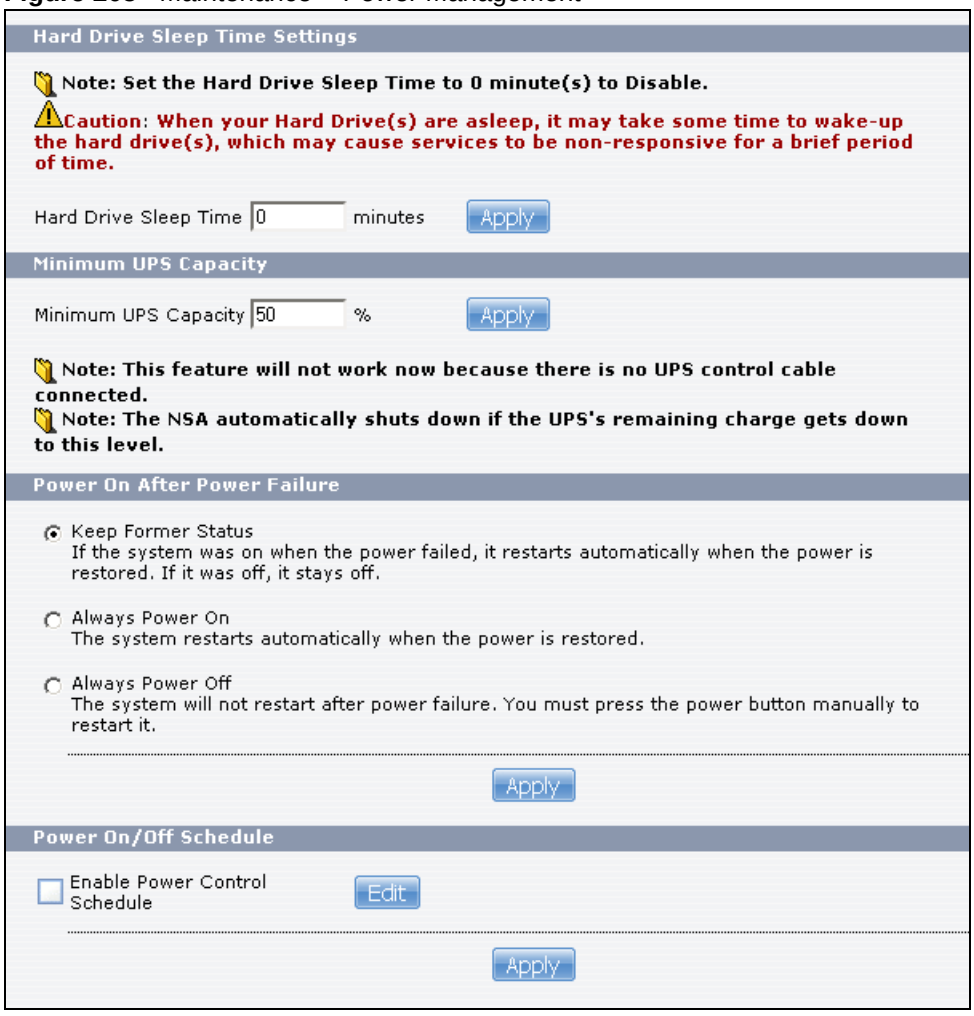
Table 105 Maintenance > FW Upgrade

LABEL	DESCRIPTION
Firmware File	Enter the location of the firmware file you want to upload.
Browse	Click this open a **Browse** dialog box to find the file on your computer if you don't want to manually enter the location.
Upload	Click this to upload the new firmware. The NSA automatically restarts after you upgrade. Wait until the restart completes before accessing the NSA again. If you interrupt the upgrade, then the NSA may become unusable.
Reset	Click this to begin configuring this screen afresh.

11.6 Power Management

Click **Maintenance** > **Power Management** to open this screen, where you can set the NSA's power management settings.

Figure 205 Maintenance > Power Management


Hard Drive Sleep Time Settings
Note: Set the Hard Drive Sleep Time to 0 minute(s) to Disable.
Caution: When your Hard Drive(s) are asleep, it may take some time to wake-up the hard drive(s), which may cause services to be non-responsive for a brief period of time.
Hard Drive Sleep Time 0 minutes
Apply
Minimum UPS Capacity
Minimum UPS Capacity 50 %
Apply
Note: This feature will not work now because there is no UPS control cable connected.
Note: The NSA automatically shuts down if the UPS's remaining charge gets down to this level.
Power On After Power Failure
Keep Former Status
If the system was on when the power failed, it restarts automatically when the power is restored. If it was off, it stays off.
Always Power On
The system restarts automatically when the power is restored.
Always Power Off
The system will not restart after power failure. You must press the power button manually to restart it.
Apply
Power On/Off Schedule
Enable Power Control Schedule
Edit
Apply

The following table describes the labels in this screen.

Table 106 Maintenance > Power Management

LABEL	DESCRIPTION
Hard Drive Sleep Time Settings	
Hard Drive Sleep Time	Enter the number of minutes the NSA will sit idle before spinning the hard disks down to sleep.
Apply	Click this to save your changes in this section.
Minimum UPS Capacity	
Minimum UPS Capacity	When you use an APC Uninterruptible Power Supply (UPS) with a USB connection to the NSA, the NSA shuts itself down if the APC UPS's battery charge gets down to the percentage you specify in this field. This allows the NSA to shut down properly and avoid data loss caused by a power failure when the UPS stops supplying power. A setting around 50% is recommended. A setting close to 100% is not recommended since it would cause the NSA to shut down whenever the UPS is charging. A setting close to 0 is also not recommended since the UPS would not have enough power to allow the NSA to shutdown properly.
Apply	Click this to save your changes in this section.

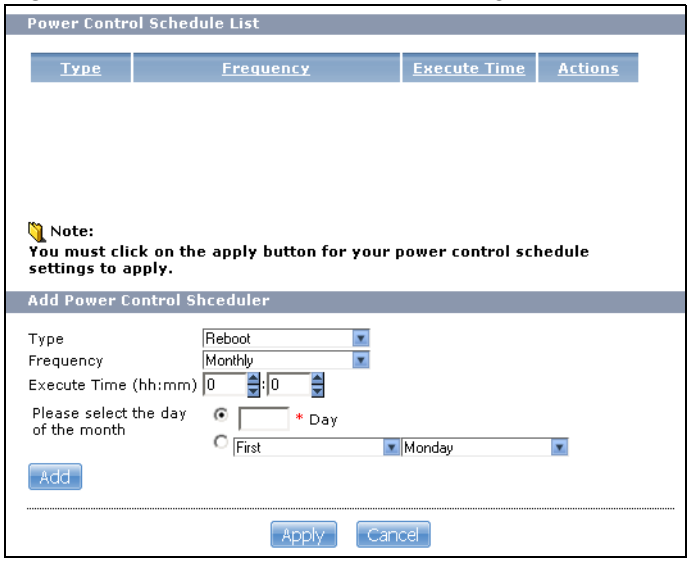
Table 106 Maintenance > Power Management (continued)

LABEL	DESCRIPTION
Power On After Power Failure	Select an option to set whether or not the NSA restarts when the power is restored after a power failure.
Keep Former Status	Select this option to have the NSA automatically restart only if it was operating when the power failed. The NSA remains off if it was already off when the power failed.
Always Power On	Select this option to keep the NSA operating as much of the time as possible. The NSA restarts automatically even if it was turned off when the power failed.
Always Power Off	Select this option to keep the NSA from automatically restarting when the power is restored after a power failure. This is a computer's "traditional" behavior. Select this if you have other servers such as a domain controller or DNS server that you want to start or check after a power failure before the NSA turns on.
Apply	Click this to save your changes in this section.
Power On/Off Schedule	
Enable Power Control Schedule	Select this option to have the NSA turn itself off and on or reboot according to the schedules you configure. Click **Edit** to go to the screen where you can configure the power control schedules.
Apply	Click this to save your changes in this section.

11.6.1 Power Control Schedule

Click **Maintenance** > **Power Management** > **Edit** to open this screen, where you can configure power control schedules to have the NSA turn on, turn off, or reboot at specified times.

Figure 206 Maintenance > Power Management > Edit



The following table describes the labels in this screen.

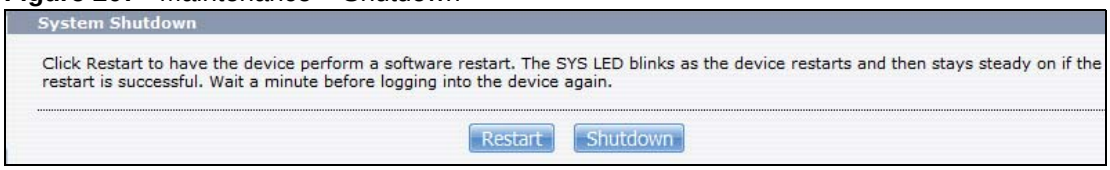
Table 107 Maintenance > Power Management > Edit

LABEL	DESCRIPTION
Power Control Schedule List	This table lists the power on, power off, and reboot schedules. For example, you could have one schedule to turn the NSA on every morning, at 8:00, another schedule to turn it off every evening at 18:00, and a third schedule to have it reboot every Friday at 14:00. Click a column's heading cell to sort the schedules by that column's criteria. Click the heading cell again to reverse the sort order.
Type	This field displays whether the power control schedule has the NSA turn on, turn off, or reboot.
Frequency	This field shows how often (monthly, weekly, or daily) the NSA is to apply this power control schedule.
Execute Time	This field shows when the NSA is to use this power control schedule (when the NSA is to turn on, turn off, or reboot).
	Delete Click this to remove a power control schedule from the list.
Add Power Control Schedule	Use this part of the screen to configure power on, power off, and reboot times.
Type	Select whether this power control schedule has the NSA turn on, turn off, or reboot.
Frequency	Select whether the NSA is to apply this power control schedule entry on a monthly, weekly, or daily basis.
Execute Time	Enter the time, day, and/or day of the month as appropriate for this power control schedule entry. Leave more than 10 minutes between the execution times of the entries. If the NSA turns off or restarts while a user is transferring files to or from the NSA, the transfer fails. The user will need to restart the transfer. The NSA skips a scheduled restart or power off if the execution time comes while the NSA is doing any of the following: • Resynchronizing a RAID • Upgrading firmware • Replacing the configuration file The NSA delays a scheduled restart or power off until it finishes any of the following: • Backing up files • Restoring files from a backup • Taking a snapshot If the NSA is turned off at the time when a restart or power off is scheduled, the NSA does not perform the restart or power off. If the NSA is turned on at the time when a power on is scheduled, the NSA does not perform the power on.
Add	Click this to add the power control schedule to the list.
Apply	Click this to save your changes.
Cancel	Click this to discard changes and close the window.

11.7 Shutdown

Click **Maintenance** > **Shutdown** to open the shutdown screen. Use this screen to turn off the NSA or restart it. Before shutting down or restarting, check the **System Status** screen to make sure that no one is logged into the NSA or transferring files to or from it.

Figure 207 Maintenance > Shutdown


System Shutdown
Click Restart to have the device perform a software restart. The SYS LED blinks as the device restarts and then stays steady on if the restart is successful. Wait a minute before logging into the device again.
Restart
Shutdown

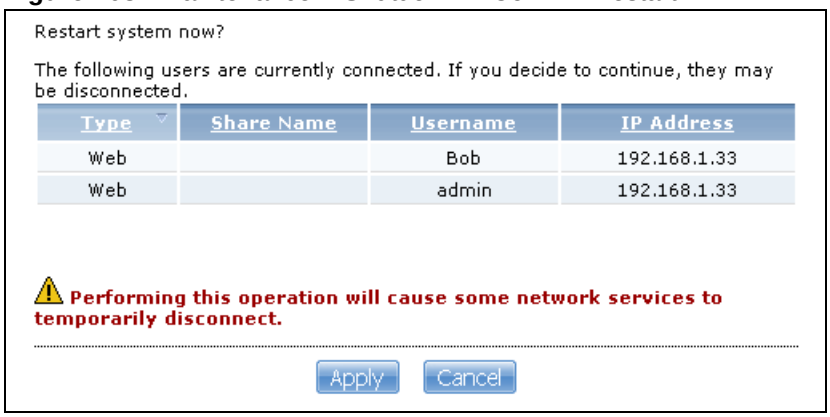
The following table describes the labels in this screen.

Table 108 Maintenance > Shutdown

LABEL	DESCRIPTION
Restart	Click this to restart the device.
Shutdown	Click this to shut down the system and restart it again later.

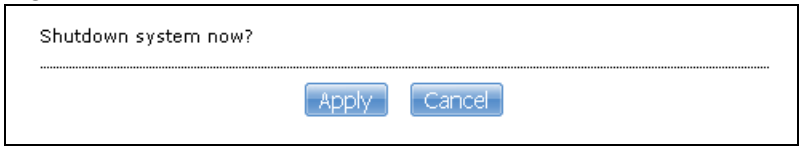
When you click the **Restart** button a pop-up screen appears asking you to confirm the action. Click **Apply** to continue or **Cancel** to abort the process.

Figure 208 Maintenance > Shutdown > Confirm Restart



When you click the **Shutdown** button a pop-up screen appears asking you to confirm. Click **Apply** to continue or **Cancel** to abort the process.

Figure 209 Maintenance > Shutdown > Confirm Shutdown



PART III
Troubleshooting and Specifications

Troubleshooting (249)
Product Specifications (257)

12

Troubleshooting

12.1 Troubleshooting Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- NSA Login and Access
- Users Cannot Access the NSA
- Backups and Snapshots
- External USB Disks

12.2 Power, Hardware Connections, and LEDs

The NSA **PWR** LED does not turn on (no LEDs are on).

- Make sure the NSA is turned on.
- Make sure you are using the power adaptor or cord included with the NSA.
- Make sure the power adaptor or cord is connected to the NSA and plugged in to an appropriate power source. Make sure the power source is turned on.
- Turn the NSA off and on.
- Disconnect the power cord for at least 10 seconds. Reconnect it and turn the NSA back on.
- If the problem continues, contact the vendor.

The NSA **SYS** LED is (quickly) flashing red.

If the **SYS** LED is quickly flashing red then a RAID array is degraded. Degraded means one of the disks in a RAID array is down but the array can still be used (if you're using RAID 1 or RAID 5). Go to the **Storage** > **Internal Storage** > **Disk** screen to identify the faulty disk. Replace the faulty disk with another of equal or greater capacity. See your Quick Start Guide for information on replacing a disk and also Disk Replacement Restrictions on page 128.

After replacing the disk, go to the **Storage** > **Internal Storage** > **RAID** screen. If the array's status is not **Resynching**, select the array and click the **Repair** icon.

The NSA **SYS** LED is orange or is flashing orange.

- If the **SYS** LED is steady on orange, then the NSA is unlocking an encrypted volume or there are no volumes in the NSA. If there are no volumes on the NSA, you cannot create shares on the NSA. You must first create a RAID and volume (you must already have an internal disk installed). See also Chapter 6 on page 125.
- If the **SYS** LED is flashing orange, then firmware is being upgraded to the NSA. Wait until the firmware upgrade is complete and the **SYS** LED turns steady green.

The disk drive **PWR** LED is off.

- Check that the NSA is on (see Power, Hardware Connections, and LEDs)
- Remove the disk tray and make sure:
  - it is a SATA I or SATA II compatible hard drive
  - it is installed correctly in the disk tray. Push the tray back into NSA disk bay until it snaps into place and push the latch up (see the NSA Quick Start Guide).
  - the hard disk is not faulty. You could either try a different hard disk or test the original hard disk in a different NSA or computer.
- If the problem continues, contact the NSA vendor.

The disk drive **ALM** LED is on.

- The hard disk has a problem. Go to the **Storage** > **Internal Storage** > **Disk** screen, select the disk and click the **S.M.A.R.T.** icon to see status details about the disk.
- If the hard disk is faulty, replace it. See your Quick Start Guide for information on replacing a disk and also Disk Replacement Restrictions on page 128. After replacing the disk, go to the **Storage** > **Internal Storage** > **Disk** screen and check the status of the new disk. You should also go to the **Storage** > **Internal Storage** > **RAID** screen and check the array's status. If it is **Resynching**, the NSA is repairing the RAID array. If it is **Degraded**, select the array and click the **Repair** icon. If the status is **Down**, recreate the array, volumes, and sharing configuration.
- If the problem continues, contact the NSA vendor.

A LAN LED is off.

- Make sure the Ethernet cable is connected properly to the NSA and connected to another (Ethernet) device. Make sure the other device is turned on. If it's connected directly to a computer, make sure that the computer network card is working (ping 127.0.0.1 on the computer).
- Use another Ethernet cable. If you're connecting to a Gigabit Ethernet, make sure you're using an 8-wire Ethernet cable.
- If the problem continues, contact the vendor.

See Section 1.1.1 on page 32 for a description of NSA LEDs.

I hear a buzzer sound coming from the NSA.

- By default when the NSA generates an emergency log, it also sounds an audible alarm to warn you.
- Log into the Web Configurator. You will be presented with a screen that displays the log and lets you disable the buzzer.

12.3 NSA Login and Access

I forgot the IP address for the NSA.

- 192.168.1.3 is the default **LAN1** IP address and 192.168.100.1 is the default **LAN2** IP address.
- Use the NDU (NSA Discovery Utility) to discover your NSA. If you have admin privileges, you can directly change the IP address of the NSA using the NDU.
- If you changed the default password and you don't have the NDU, use the **RESET** button at the front of the NSA. Refer to Section 2.7 on page 52 for detailed information on the reset button.

I forgot the password.

- The default password is **1234**.
- You may have to reset the NSA password or configuration - see Section 2.7 on page 52 for detailed information on the reset button.

The NDU cannot discover my NSA.

- Confirm that the computer running the NDU has a network connection. See the section on the NSA's LAN connection for related information.
- The computer running the NDU can only discover NSAs in the same subnet. NSAs connected to the same switch or router as your NDU computer are usually in the same subnet unless the router is doing subnetting or the switch is implementing VLAN.
- The Genie Backup program uses the same network port as the NDU to discover the NSA. To avoid a port conflict, do not run the Genie Backup Manager at the same time as the NDU.

A non-admin user wants to change her password.

Non-admin users can change their passwords directly. See Section 2.5.7 on page 46 for details on how to do that.

I cannot see or access the **Login** screen in the Web Configurator.

- Make sure you are using the correct IP address.
  - 192.168.1.3 is the default **LAN1** IP address and 192.168.100.1 is the default **LAN2** IP address.
  - If you changed the IP address, use the new IP address.
  - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for "I forgot the IP address for the NSA." on page 251.
- Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.1.1 on page 32.
- Make sure your Internet browser has JavaScripts and Java enabled.
- Make sure your computer is in the same subnet as the NSA.
- Reset the NSA to its factory defaults, and try to access the NSA with the default IP address. See Section 2.7 on page 52 for detailed information on the reset button.
- If the problem continues, contact the network administrator or vendor.

I can see the **Login** screen, but I cannot log in to the NSA.

- Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- Turn the NSA off and on.
- If this does not work, you have to reset the device to its factory defaults. See Section 2.7 on page 52 for detailed information on the reset button.

12.4 Users Cannot Access the NSA

A local user cannot access a share

- Check that the NSA is turned on and connected to the network. The local user should try to ping the NSA or use the NDU to discover it.
- The local user should check that he entered his login name and password correctly.
- Check if the share exists and has the correct access settings for this user.
- Check the Access Control List (ACL) of read/write permissions associated with specific files and/or folders. Account names added to the list are linked to the files and folders that they are allowed to access, along with what kinds of actions they are allowed to perform with those files and folders (delete, move, rename, and so on).
- The user's computer may already be connected to another of the NSA's shares using a different user name and/or password. This can happen without the user realizing it if the user's computer automatically connects to a share at logon. Right-click any other connected shares and click **Disconnect**. Then re-attempt to connect to the desired share.
- Check if the share has an ANONMYOUS or EVERYONE access right. If the user is already logged into a share using her username and password, she will NOT be able to access a share that has ANONYMOUS FTP only access rights (as these require 'no login'). In this case she should log out and try to access the share again without logging in. See Section 8.4.2.3 on page 193 for more details.
- Check if the shared folder is a subfolder of another (parent) share. Check that the parent share's access rights do not conflict with the subfolder share. It is recommended that you do not create subfolder shares.
- Check if the user belongs to a group with conflicting access rights. **DENY** always takes precedence. If you allow a user **FULL** access to a share but set his group to **DENY**, then he will NOT be able to access the share.
- The local user should check if there are any existing mapped network drives to the NSA. He may need to disconnect existing CIFS connections as new CIFS connection may use previously-saved login information that may be different to NSA login.
- Check that the array in which the share resides, exists and is not down or degraded. If the array is down or degraded, see Section 12.2 on page 249.
- If the user is using DFS links, then he can only access the NSA using CIFS and not FTP.
- Check that the share has not been disabled.

I cannot import domain user or user group information even though testing of the connection to the domain controller is OK.

- Check the NSA's DNS setting. The DNS server the NSA is using must be able to resolve the domain controller's address. If the domain controller uses a private IP address, the NSA needs to use a private DNS server. If the domain controller uses a public IP address, the NSA needs to use a public DNS server.

- Leave the domain and re-join it.

A domain user can't access a share.

In addition to the checks listed previously for local users, check that the domain controller is turned on and connected to the network.

A user can access a share but cannot access individual folders or files within the share.

Check the Access Control List (ACL) of read/write permissions associated with the share's specific files and/or folders. Account names added to the list are linked to the files and folders that they are allowed to access, along with what kinds of actions they are allowed to perform with those files and folders (delete, move, rename, and so on).

12.5 Backups and Snapshots

I cannot make a backup.

- Check the logs to find the reason why the backup failed.
- You can also look at the **Backup** screen's **Last Run Result** display.
- If you're backing up to another NSA, another NSA, or a computer, check that it allows the NSA to write files to it. For a synchronization backup, the target must be another NSA or another compatible model.
- Check that enough space is available on the external disk. If there isn't you may need to purge older backups or delete other files on the backup USB disk or NSA (see Section 9.2.3 on page 208).
- Check that the NSA is not performing another backup job. **Scheduler** queues backups when a different backup is already going on at the time a backup is scheduled.

I cannot take a snapshot

- Check the logs. The NSA generates an alert log when an error occurs during the snapshot capture process. This log lists why the snapshot failed, for example, low disk space.

You may need to manually delete some previous snapshots to make more space. If you still cannot take the snapshot you may need to recreate the volume with a larger amount of space reserved for snapshots.

- You can also check the logs on the NSA to find out the reason why the snapshot failed.
- A snapshot must be done on a complete volume. Check that the volume is not down, locked, or degraded. If it is, then see Section 12.2 on page 249.

The snapshot or backup does not run at the time configured.

- Check that the correct time is configured on the NSA.
- Check that the NSA is able to access the time server from which it gets the time; see Chapter 5 on page 121.

12.6 External USB Disks

The **COPY** LED is red.

Copying files from a USB device failed. The USB device may not be compatible with the NSA. Press the **COPY** button to set the **COPY** LED back to green. Try saving the files onto a computer and then from the computer to the NSA (through the network connection).

13

Product Specifications

See also the Getting to Know Your NSA chapter for a general overview of the key features.

13.1 Feature Tables

These are the main external physical features.

Table 109 Physical Features

2 USB Ports	Expand storage capacity by attaching compatible USB (version 2) hard drives to the USB ports.
2 Gigabit Ethernet Ports	The 10/100/1000 Mbps auto-negotiating Ethernet ports allow the NSA to detect the speed of incoming transmissions and adjust appropriately without manual intervention. They allow data transfers of either 100 Mbps or 1000 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network. Use 8-wire Ethernet cables for Gigabit connections. The ports are also auto-crossover (MDI/MDI-X) meaning it automatically adjusts to either a crossover or straight-through Ethernet cable.
SATA Interface	Serial ATA is an interface technology that allows high speed data transfer. Serial ATA also allows more efficient internal airflow and also smaller chassis design.
Hot Swappable Hard Drives	You can remove and install hard drives while the NSA is operating.
Buzzer	Audible alarm buzzer triggered by logs of a user-specified severity level.
Reset Button	Use the reset button to reset the NSA (user name to “admin”, default password to “1234”, default IP address to 192.168.1.3 with subnet mask of 255.255.255.0) or restore the factory default configuration file (all configurations, including shares, users, passwords and so on are returned to the original configurations).

These are some of the main firmware features of the NSA.

Table 110 Firmware Features

Hard Drive Arrays	RAID 0 with 2,3, or 4 hard drives. RAID 1 with 2 hard drives RAID 5 with 3 or 4 hard drives RAID 10 (1+0) with 4 hard drives JBOD with 1,2,3, or 4 hard drives
Backup	Create separate archive backups or synchronize a copy.
Snapshot	A snapshot is a backup of your NSA data on the NSA. If files within a volume become infected or corrupted, you can revert the volume back to a previous snapshot. It’s a good idea to create a snapshot before backing up data, to be sure you’re backing up consistent data even if the backup is still running several hours later.

Table 110 Firmware Features (continued)

Disk Quota	Use the disk quota feature to stop one user(s) from using up all disk capacity by setting a limit on how much storage space he/she may use.
User Passwords	Configure a password for an individual **User** to restrict access to the NSA. Non-admin users can change their own passwords by accessing the Web Configurator. The **Change Password** screen appears when a username other than “admin” is entered.
Volume Encryption	The NSA can create encrypted volumes so an attacker who removes the physical drive still cannot read the data.
ACL	The Access Control List (ACL) defines user read/write permissions for specific files and/or folders.
Storage Event Logs	The NSA can keep detailed records of all user access to files and folders.
Workgroup and Domain Security Modes	For Windows or Mac OSX users (using the Common Internet File System (CIFS) protocol for remote file access) you can configure **Workgroup** mode requiring users to log in with a user name and password. These user and group accounts are maintained on the NSA. For a large number of CIFS users where accounts are stored on an external server, you can use **Domain** security mode (Primary Domain Controller)
Client Support	Data can be shared among all Windows, Mac, Linux, and UNIX users that have FTP client software or CIFS file sharing support (such as Samba for Linux and UNIX users).
IEEE 802.3d Ethernet Failover	LAN2 can backup LAN1. If LAN1 loses its connection, LAN2 takes over LAN1’s IP address and traffic.
IEEE 802.3d Ethernet Load Balance	The NSA can distribute the traffic load across LAN1 and LAN2.
HTTP/HTTPS	Access the NSA using a regular web connection (HTTP) or an encrypted web connection (HTTPS) using secure socket layer (SSL).
SSL Certificate Manager	The NSA can generate certificates and certificate requests.
DHCP (Dynamic Host Configuration Protocol)	DHCP (Dynamic Host Configuration Protocol) allows the NSA to obtain an IP address and subnet mask at start-up from a centralized DHCP server. Alternatively, you can give the NSA a static IP address and subnet mask.
Full Network Management	The embedded Web Configurator is an platform-independent web-based utility that allows you to easily access the NSA’s management settings.
Firmware Upload and Configuration File Management	Upload new firmware to the NSA using the Web Configurator. You can also back up and restore the NSA configuration file containing all its settings to/from your computer.
NSA Discovery Utility (NDU)	Use the NDU from a Windows computer to find NSA(s) in your network, access the NSA login page, change its IP address configuration or map to a Windows network drive.
Genie Backup Manager	Genie Backup Manager is a tool for Windows users to create (and schedule) backups of data stored on their Windows computer to an NSA.
S.M.A.R.T.	The NSA can use the S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) monitoring system to detect and report on hard drive reliability indicators to help anticipate hard drive failures.

Table 110 Firmware Features (continued)

UPS Integration	Connect an APC Uninterruptible Power Supply (UPS) with a USB connection to the NSA. The NSA shuts itself down if the UPS's battery charge gets down to a user-configurable percentage. This allows the NSA to shut down properly and avoid data loss caused by a power failure when the UPS stops supplying power.
Hard Disk Drive Power Saving	If a hard disk inside the NSA for a user-configurable period of time, the NSA puts it to sleep until you use it again.
Power Control Schedule	The NSA can turn itself off and on or restart according to the schedule you configure.
Auto Shutdown	The NSA automatically turns itself off when there is almost no power or the temperature is too high.
Time and Date	Configure a time server and set a time zone for your NSA to show the correct times in e-mail alerts and logs.
E-mail Alerts	Configure an e-mail to be sent to an NSA administrator whenever an error occurs or as a scheduled log summary.

13.2 Specification Tables

The NSA hardware specifications are shown in the following table.

Table 111 NSA Hardware Specifications

LAN1 IP Address	192.168.1.3 if the NSA cannot get an IP address from a DHCP server.
LAN2 IP Address	192.168.100.3 if the NSA cannot get an IP address from a DHCP server.
Subnet Mask	255.255.255.0 (24 bits) if the NSA cannot get a subnet mask from a DHCP server.
Default Username	admin
Default Password	1234
Dimensions	140(W)*300(D)*305(H) mm
Weight	6.2 kg
Disk Trays	Four
Compatible Hard Disks[A]	SATA II (Serial Advanced Technology Attachment) hard disk serial links The NSA also recognizes SATA I compatible drives.
USB	The USB devices can use a combined total current of no more than 500 mA from the NSA. Use an external power adaptor if more current is necessary.
Printers	Connect up to a maximum of 2 USB printers to the NSA.
UPS	The NSA supports APC Uninterruptible Power Supply
CPU	Freescale 8543 (800MHz/ 400 MHz DDR SDRAM)
CPU Operating Temperature	0^{O} to 85^{O} C
Ports	
Ethernet	Two auto-negotiating, auto MDI/MDI-X 10/100/1000[B] Mbps RJ-45 Ethernet ports (10 Base-T/100 Base-TX/1000 Base-T)
USB v2.0 Storage	Two ports on the front panel. Windows: NTFS (read only), FAT32 and FAT16 Linux: EXT2, EXT3 and XFS
LEDs	PWR, SYS, LAN1, LAN2, and COPY

Table 111 NSA Hardware Specifications (continued)

Reset Button	Reset the NSA or restore the factory default configuration file
AC Input	Voltage: 100 - 240 V at 50 - 60 Hz Current: 2 A
DC Output	Voltage: 19 V Current: 2 A
Operating Temperature	0º C ~ 40º C
Storage Temperature	-30º C ~ 60º C
Operating Humidity	20% ~ 90% RH (non-condensing)
Storage Humidity	20% ~ 95% RH (non-condensing)
Certifications	EMC: FCC Class B, EN 55022 Class B Safety: UL 60950-1, CSA 60950-1, EN60950-1, IEC 60950-1

A. Hard drives may not be included with your NSA.

B. Use an 8-wire Ethernet cable for Gigabit connections.

The NSA firmware specifications are shown in the following table

Table 112 NSA Firmware Specifications

File Storage System	SINGLE, RAID 0, 1, 5
Network Protocols	TCP/IP, UDP/IP DHCP Client FTP HTTP/ HTTPS
File Management	Distributed File System (DFS) Create/Delete System Volume
Network File Sharing Protocol	CIFS/SMB for Windows and Mac OSX HTTP for web browser FTP NFS
Network Security	Authentication Share level Active Directory Services (ADS) Encrypted Network Login
Supported Clients	Windows 2000 Professional/Server Windows XP Home/Professional Windows Me Linux
Max no. of user accounts	512[A]
Maximum number of concurrent FTP sessions	60[A]
Maximum number of concurrent CIFS sessions	60[A]
Maximum number of snapshots in the NSA	20
Maximum number of snapshots per volume	5

Table 112 NSA Firmware Specifications (continued)

System Management	Remote Management via Web Configurator (HTTP) Secure Remote Management via Web Configurator (HTTPS) NSA Discovery Utility (NDU) E-mail alerts
Logging/Monitoring	Centralized Logs
Firmware Upgrade	Web Configurator
Web Browsers Supported	Internet Explorer 6.0 and later versions. Firefox 1.07 and later versions.

A. Limits may vary depending on user-share resource usage.

13.3 Power Consumption

The NSA-2400 was tested using the specified power sources with the external power adapter and with four hard drives installed.

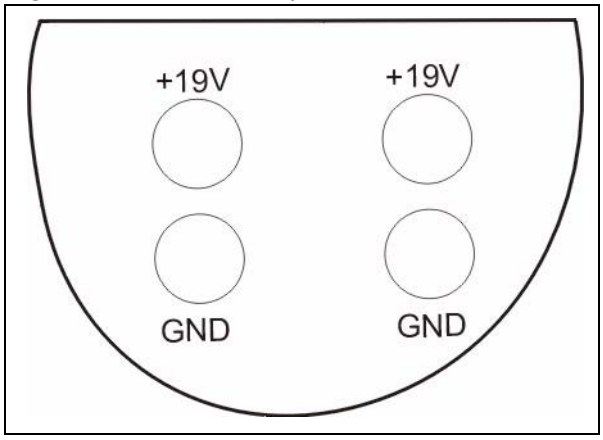
This table is a laboratory test of NSA-2400 power consumption for your reference only.

Table 113 Power Consumption in Watts (W)

POWER SOURCE	SYSTEM BOOT UP	SYSTEM READ/WRITE	SYSTEM IDLE (HARD DISKS IN POWER SAVING MODE)
240V/50Hz	77.8 (peak)	51.6 (peak)	24.2
120V/60Hz	76.5(peak)	52.9 (peak)	23.0
100V/60Hz	76.0 (peak)	53.1 (peak)	22.5

This is the external power adaptor pinout specification

Figure 210 Power Adaptor Pinout.



PART IV Appendices and Index

Log Messages (265)
Setting Up Your Computer's IP Address (275)
Importing Certificates (299)
Open Source Licences (323)
Legal Information (353)
Index (355)

A

Log Messages

This appendix shows some NSA log messages.

Log Messages

Table 114 Log Messages

FEATURE	SEVERITY	MESSAGE	ARGUMENT(S)			
Action Log	INFO	[ClientIP][UserName][ShareName][ServiceName][ActionName][FilePath+FileName_Under the share]	ServiceName: FTP/CIFS/ WEB	ActionName: Delete, Delete DIR, Create DIR, Write (upload), Read (download)		
Action Log: Rename	INFO	[ClientIP][UserName][ShareName][ServiceName][Rename][FilePath+FileName_Under the share]->[FilePath+FileName_Under the share]	ServiceName: FTP/CIFS/ WEB			
CIFS - domain	INFO	Join domain {0} (type: {1}) success	Domain Name	Domain Type		
CIFS - domain	INFO	Leave Domain success.				
CIFS - domain	INFO	Import Domain User and Group success: {0} user(s), {1} group(s). It took {2} seconds.	number of domain user	number of domain group	number of seconds to take when import domain user and group	
CIFS - domain	INFO	Import Domain User and Group Description success: {0} user(s), {1} group(s).	number of domain user description	number of domain group description		
CIFS - share	NOTICE	Add new share {0}.	Share Name			
CIFS - share	NOTICE	Delete share {0}.	Share Name			
CIFS - share	NOTICE	Add new disabled share {0} for unshared folder: {1} in volume: {2}.	Share Name	Folder Name	Volume Name	
CIFS - share	NOTICE	Recycle-bin disabled. Remove recycle-bin folder in share: {0}.	Share Name			

Table 114 Log Messages

FEATURE	SEVERITY	MESSAGE	ARGUMENT(S)			
CIFS - share	NOTICE	Purge all files in recycle-bin folder in share: {0}.	Share Name			
CIFS - share	INFO	Expire recycle-bin finish for share {0}, process time: {1} seconds, remove {2} file ({3} bytes)	Share Name	How log it takes to process this recycle bin	Number of files removed in recycle bin	Number of bytes removed in recycle bin
CIFS - user	NOTICE	Add new user {0} by {1} from {2}.	User Name	User Name	IP	
CIFS - user	NOTICE	Delete new user {0} by {1} from {2}.	User Name	User Name	IP	
CIFS - user	NOTICE	The user {0} from {1} has attempted to change the user {2} password but old password verification fail.	User Name	IP	User Name	
CIFS - user	NOTICE	User {0} password has been changed by {1} from {2}.	User Name	User Name	IP	
CIFS - group	NOTICE	Add new group {0}.	Group Name			
CIFS - group	NOTICE	Delete group {0}.	Group Name			
COPY BTN	NOTICE	Copy Button : Can not get configuration for Copy Button				
COPY BTN	NOTICE	Copying content of {0} to {1}: Start	USB / Internal Path	USB / Internal Path		
COPY BTN	NOTICE	Copying content of {0} to {1}: Failed	USB / Internal Path	USB / Internal Path		
COPY BTN	NOTICE	Copying content of {0} to {1}: Done	USB / Internal Path	USB / Internal Path		
FTP	INFO	USER {0} ({1}) login FTP success	User Name	IP		
FTP	INFO	USER {0} ({1}) logout FTP	User Name	IP		
FTP	INFO	USER {0} ({1}) login FTP failed	User Name	IP		
FTP	NOTICE	FTP service starts				
FTP	NOTICE	FTP service stops				
FTP	NOTICE	FTP service starts with TLS mode				
LOG	INFO	Clean system log complete				
LOG	INFO	Change DB path to {0}/log OK	Share Name			
LOG	INFO	Reset DB to System Default OK				
Network	NOTICE	Network Config setting is changed				
Network	NOTICE	Network interface {0} link up	Network interface name			

Table 114 Log Messages

FEATURE	SEVERITY	MESSAGE	ARGUMENT(S)			
Network	NOTICE	Network interface {0} link down				
NFS	INFO	Enable NFS: SUCCESS				
NFS	CRIT	Enable NFS: FAILED				
NFS	INFO	Disable NFS: SUCCESS				
NFS	CRIT	Disable NFS: FAILED				
NFS	INFO	Export {0} ({1},{2}) to NFS: SUCCESS	Path	IP Filter	Permission: rw, ro	
NFS	CRIT	Export {0} ({1},{2}) to NFS: FAILED	Path	IP Filter	Permission: rw, ro	
NFS	INFO	Remove All data in NFS Share {0}: SUCCESS	NFS Share Name			
NFS	CRIT	Remove All data in NFS Share {0}: FAILED	NFS Share Name			
RESET BTN	NOTICE	RESET BUTTON: Reset admin password & ip setting				
RESET BTN	NOTICE	RESET BUTTON: Reset configuration to factory default.				
Scheduler	INFO	Job {0} is triggered by schedule	JOB name			
Scheduler	INFO	Job {0} is triggered by user	JOB name			
Scheduler	ERR	Job {0} is resulted as failed	JOB name			
Scheduler	INFO	Job {0} is is finished successfully	JOB name			
Scheduler	INFO	Job {0} is canceled by user	JOB name			
Scheduler	INFO	Restore job [{0}] is triggered by user	JOB name			
Scheduler: Power	INFO	[Power On] schedule is triggered.				
Scheduler: Power	INFO	[Power Off] schedule is triggered.				
Scheduler: Power	INFO	[Reboot] schedule is triggered.				
Snapshot	INFO	Take Snapshot with Job Name {0} (Rotate Count={1}): SUCCESS	Snapshot Job name	Rotate Count		
Snapshot	CRIT	Take Snapshot with Job Name {0} (Rotate Count={1}): FAILED	Snapshot Job name	Rotate Count		
Snapshot	INFO	Purge Snapshot Image {0}: SUCCESS	Snapshot Image Name			
Snapshot	CRIT	Purge Snapshot Image {0}: FAILED	Snapshot Image Name			
Snapshot	INFO	Delete Snapshot Image {0}: SUCCESS	Snapshot Image Name			
Snapshot	CRIT	Delete Snapshot Image {0}: FAILED	Snapshot Image Name			

Table 114 Log Messages

FEATURE	SEVERITY	MESSAGE	ARGUMENT(S)			
Snapshot	INFO	Expand Snapshot Image {0}(Increased Size={1}MB): SUCCESS	Snapshot Image Name	Size		
Snapshot	CRIT	Expand Snapshot Image {0}(Increased Size={1}MB): FAILED	Snapshot Image Name	Size		
Snapshot	INFO	Enable Snap-Share: SUCCESS				
Snapshot	CRIT	Enable Snap-Share: FAILED				
Snapshot	INFO	Disable Snap-Share: SUCCESS				
Snapshot	CRIT	Disable Snap-Share: FAILED				
Snapshot	CRIT	No Freespace to Expand Snapshot. Purge Snapshot Image {0} to Increase Freespace.	Snapshot Image Name			
Snapshot	CRIT	The following snapshot is invalid:{0}. Its snapshot size is {1}MB.	Snapshot name	Size		
Storage - Disk	INFO	Disk{0} is plugged				
Storage - Disk	INFO	Disk{0} is unplugged				
Storage - Disk	INFO	An external Mass Storage device is plugged.				
Storage - Disk	INFO	An external Mass Storage device is unplugged				
Storage - RAID	INFO	Create RAID (raid label={0}): Success				
Storage - RAID	INFO	Relabel RAID: Success				
Storage - RAID	INFO	Delete RAID: Success				
Storage - RAID	INFO	Start Repairing Degraded Raid: Success				
Storage - RAID	INFO	Modify Rebuild Priority to high/ normal/low: Success				
Storage - RAID	INFO	Reshape Raid5 by Adding disk{0}: Success	Disk Slog ID			
Storage - RAID	INFO	Add Hot-Spare disk{0} to Raid: Success	Disk Slog ID			
Storage - RAID	INFO	Remove Hot-Spare disk{0} from Raid: Success	Disk Slog ID			
Storage - RAID	CRIT	Create RAID (raid label={0}): FAILED				
Storage - RAID	CRIT	Relabel RAID: FAILED				
Storage - RAID	CRIT	Delete RAID: FAILED				

Table 114 Log Messages

FEATURE	SEVERITY	MESSAGE	ARGUMENT(S)			
Storage - RAID	CRIT	Start Repairing Degraded Raid: FAILED				
Storage - RAID	CRIT	Modify Rebuild Priority to high/ normal/low: FAILED				
Storage - RAID	CRIT	Reshape Raid5 by Adding disk{0}: FAILED	Disk Slog ID			
Storage - RAID	CRIT	Add Hot-Spare disk{0} to Raid: FAILED	Disk Slog ID			
Storage - RAID	CRIT	Remove Hot-Spare disk{0} from Raid: FAILED	Disk Slog ID			
Storage - RAID	EMERG	There is a RAID Degraded				
Storage - RAID	CRIT	Please check disk{0}.	Which disk to check when degrade			
Storage - RAID	NOTICE	Auto Repair Degraded RAID by disk{0}	Disk Slog ID			
Storage - RAID	NOTICE	Raid Rebuild Percentage: {0}%	20/40/60/80/ 100			
Storage - Volume	INFO	Create Internal Normal Volume [{0}] (Size={1}MB): SUCCESS	Volume Name	Size		
Storage - Volume	INFO	Create Internal Crypto Volume [{0}] (Size={1}MB) using PASSWD: SUCCESS	Volume Name	Size		
Storage - Volume	INFO	Create Internal Crypto Volume [{0}] using USB Key (Size={1}MB): SUCCESS	Volume Name	Size		
Storage - Volume	INFO	Create External Normal Volume [{0}] ({1}): SUCCESS	Volume Name	Filesystem type		
Storage - Volume	INFO	Create External Crypto Volume [{0}] ({1}) using PASSWD: SUCCESS	Volume Name	Filesystem type		
Storage - Volume	INFO	Create External Crypto Volume [{0}] using USB Key ({1}): SUCCESS	Volume Name	Filesystem type		
Storage - Volume	INFO	Delete Volume: SUCCESS				
Storage - Volume	INFO	Create USB Key: SUCCESS				
Storage - Volume	INFO	Duplicate USB Key: SUCCESS				
Storage - Volume	INFO	Rename Internal Volume to [{0}]: SUCCESS	Volume Name			
Storage - Volume	INFO	Expand Volume (Increased Size={0}MB): SUCCESS	Size			
Storage - Volume	INFO	Lock Internal Volume: SUCCESS				

Table 114 Log Messages

FEATURE	SEVERITY	MESSAGE	ARGUMENT(S)			
Storage - Volume	INFO	Unlock Internal Volume: SUCCESS				
Storage - Volume	INFO	Change Internal Crypto Volume Password Prompt to [{0}]: Success	New Password Prompt			
Storage - Volume	INFO	Change Internal Crypto Volume Password: SUCCESS				
Storage - Volume	INFO	Rename External Volume to [{0}]: SUCCESS	Volume Name			
Storage - Volume	INFO	Lock External Volume: SUCCESS				
Storage - Volume	INFO	Unlock External Volume: SUCCESS				
Storage - Volume	INFO	Change External Crypto Volume Password Prompt to [{0}]: Success	New Password Prompt			
Storage - Volume	INFO	Change External Crypto Volume Password: SUCCESS				
Storage - Volume	INFO	Start Scanning Internal Volume (read-only/read-write operation)				
Storage - Volume	INFO	Scan Internal Volume (read-only/read-write operation): SUCCESS				
Storage - Volume	INFO	Cancel Internal Volume Scan: SUCCESS				
Storage - Volume	INFO	Scan External Volume: SUCCESS				
Storage - Volume	INFO	Cancel External Volume Scan: SUCCESS				
Storage - Volume	INFO	Eject External Disk ({0}): SUCCESS	disk id			
Storage - Volume	CRIT	Create Internal Normal Volume [{0}] (Size={1}MB): FAILED	Volume Name	Size		
Storage - Volume	CRIT	Create Internal Crypto Volume [{0}] (Size={1}MB) using PASSWD: FAILED	Volume Name	Size		
Storage - Volume	CRIT	Create Internal Crypto Volume [{0}] using USB Key (Size={1}MB): FAILED	Volume Name	Size		
Storage - Volume	CRIT	Create External Normal Volume [{0}] ({1}): FAILED	Volume Name	Filesystem type		
Storage - Volume	CRIT	Create External Crypto Volume [{0}] ({1}) using PASSWD: FAILED	Volume Name	Filesystem type		
Storage - Volume	CRIT	Create External Crypto Volume [{0}] using USB Key ({1}): FAILED	Volume Name	Filesystem type		
Storage - Volume	CRIT	Delete Volume: FAILED				

Table 114 Log Messages

FEATURE	SEVERITY	MESSAGE	ARGUMENT(S)			
Storage - Volume	CRIT	Create USB Key: FAILED				
Storage - Volume	CRIT	Duplicate USB Key: FAILED				
Storage - Volume	CRIT	Rename Internal Volume to [{0}]: FAILED	Volume Name			
Storage - Volume	CRIT	Expand Volume (Increased Size={0}MB): FAILED	Size			
Storage - Volume	CRIT	Lock Internal Volume: FAILED				
Storage - Volume	CRIT	Unlock Internal Volume: FAILED				
Storage - Volume	CRIT	Change Internal Crypto Volume Password Prompt to [{0}]: FAILED	New Password Prompt			
Storage - Volume	CRIT	Change Internal Crypto Volume Password: FAILED				
Storage - Volume	CRIT	Rename External Volume to [{0}]: FAILED	Volume Name			
Storage - Volume	CRIT	Lock External Volume: FAILED				
Storage - Volume	CRIT	Unlock External Volume: FAILED				
Storage - Volume	CRIT	Change External Crypto Volume Password Prompt to [{0}]: FAILED	New Password Prompt			
Storage - Volume	CRIT	Change External Crypto Volume Password: FAILED				
Storage - Volume	CRIT	Start Scanning Internal Volume (read-only/read-write operation)				
Storage - Volume	CRIT	Scan Internal Volume (read-only/read-write operation): FAILED				
Storage - Volume	CRIT	Cancel Internal Volume Scan: FAILED				
Storage - Volume	CRIT	Scan External Volume: FAILED				
Storage - Volume	CRIT	Cancel External Volume Scan: FAILED				
Storage - Volume	CRIT	Eject External Disk ({0}): FAILED	disk id			
Storage - Volume	CRIT	Detected Disk{0} I/O error.				
System	NOTICE	Hostname is set to {0}				
System	NOTICE	System description is changed				
System	EMERG	Temperature is too high!				

Table 114 Log Messages

FEATURE	SEVERITY	MESSAGE	ARGUMENT(S)			
System	EMERG	Temperature exceeds the upper bound and may cause damage.System is going to shutdown.				
System	INFO	Temperature is back to normal.				
System	EMERG	Fan speed is too low and may cause damage				
System	ERR	Fan speed is lower than normal speed.				
System	INFO	Fan speed is normal.				
System	INFO	Device is shutdown by administrator				
System	NOTICE	The system was shutdown abnormally.				
PWR BTN	NOTICE	System is shutdown by power button				
UPS	EMERG	Remaining battery charge below limit on UPS. Doing shutdown.				
USB	NOTICE	An external APC UPS device is plugged.				
USB	NOTICE	An external APC UPS device is unplugged.				
USB	NOTICE	An external Printer device is plugged.				
USB	NOTICE	An external Printer device is unplugged.				
USB	NOTICE	An external USB hub device is plugged.				
USB	NOTICE	An external USB hub device is unplugged.				
System - FW	INFO	CGI: File uploaded. File name: {0}, file size: {1} bytes	File Name	File Size		
System - FW	INFO	The file {0} is verified and restored, system is going to restart	File Name			
System - FW	NOTICE	The file {0} is corrupted. Stop the configuration restoration.	File Name			
System - FW	NOTICE	Firmware is upgrading from version {0} to {1}	OLD_VERSION	NEW_VERSION		
System - FW	NOTICE	Firmware upgrade fails, the file is invalid or corrupted!				
System - Time	INFO	NTP server is set to {0}	NTP server			
System	INFO	NTP updates successfully from {0}	NTP server			
System - Time	INFO	Clock timezone is set to {0}	TimeZone			

Table 114 Log Messages

FEATURE	SEVERITY	MESSAGE	ARGUMENT(S)			
System - Time	INFO	Daylight saving is disabled				
System - Time	INFO	Daylight saving is enabled				
Web	INFO	USER {0} ({1}) login WEB success	User Name	IP		
Web	INFO	USER {0} has logged out from WEB	User Name			
Web	INFO	USER {0} ({1}) login WEB failed	User Name	IP		
SSL	INFO	Certficate is imported successfully.				
SSL	NOTICE	The public key in {0} doesn't match the public key of Certificate Request on system.	File Name			
SSL	NOTICE	There is not any Certificate Request and private key on system. Please create a Certificate Request and enroll it.				
SSL	NOTICE	The file {0} is not a valid Certificate file.	File Name			
SSL	NOTICE	Failed to import Certificate.				
SSL	NOTICE	Unexpected error while importing Certificate file.				

B

Setting Up Your Computer's IP Address

Your specific ZyXEL device may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

In this appendix, you can set up an IP address for:

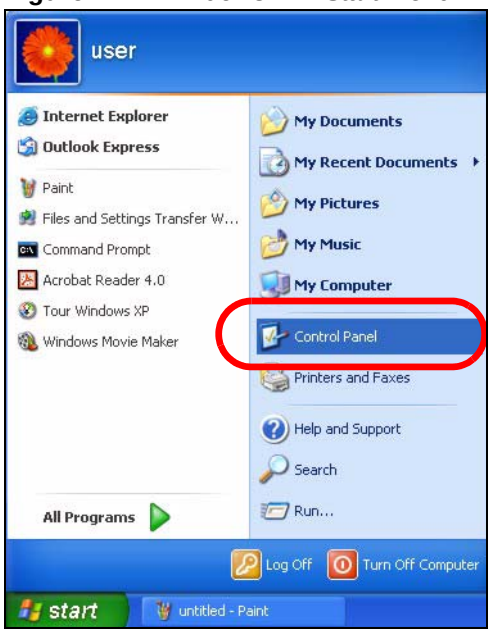
- Windows XP/NT/2000 on page 276
- Windows Vista on page 279
- Mac OS X: 10.3 and 10.4 on page 283
- Mac OS X: 10.5 on page 286
- Linux: Ubuntu 8 (GNOME) on page 289
- Linux: openSUSE 10.3 (KDE) on page 293

Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

1 Click **Start** > **Control Panel**.

Figure 211 Windows XP: Start Menu

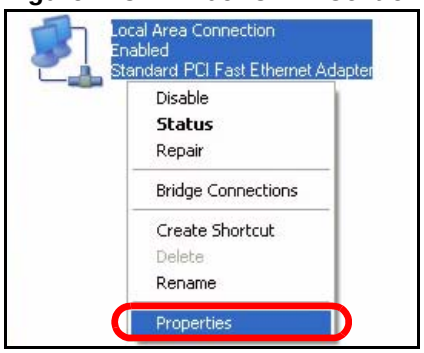


2 In the **Control Panel**, click the **Network Connections** icon.

Figure 212 Windows XP: Control Panel

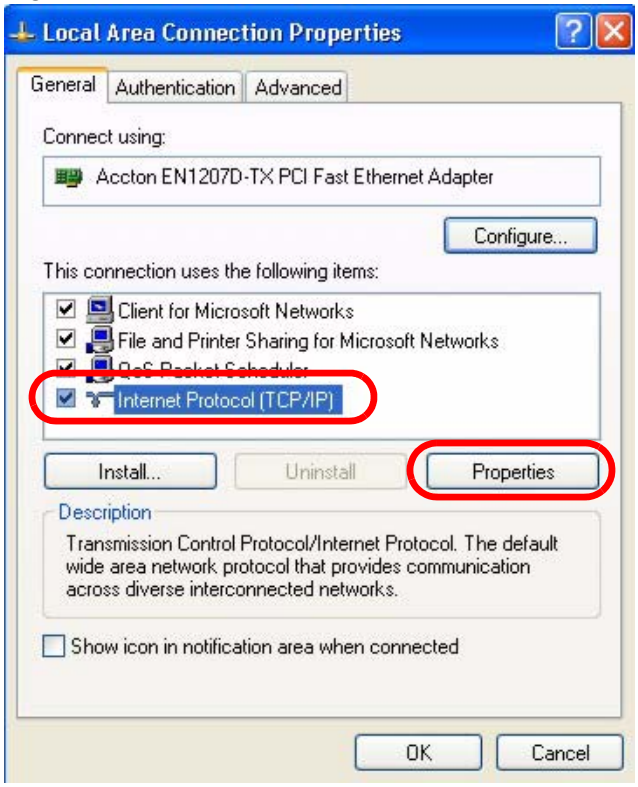
3 Right-click **Local Area Connection** and then select **Properties**.

Figure 213 Windows XP: Control Panel > Network Connections > Properties



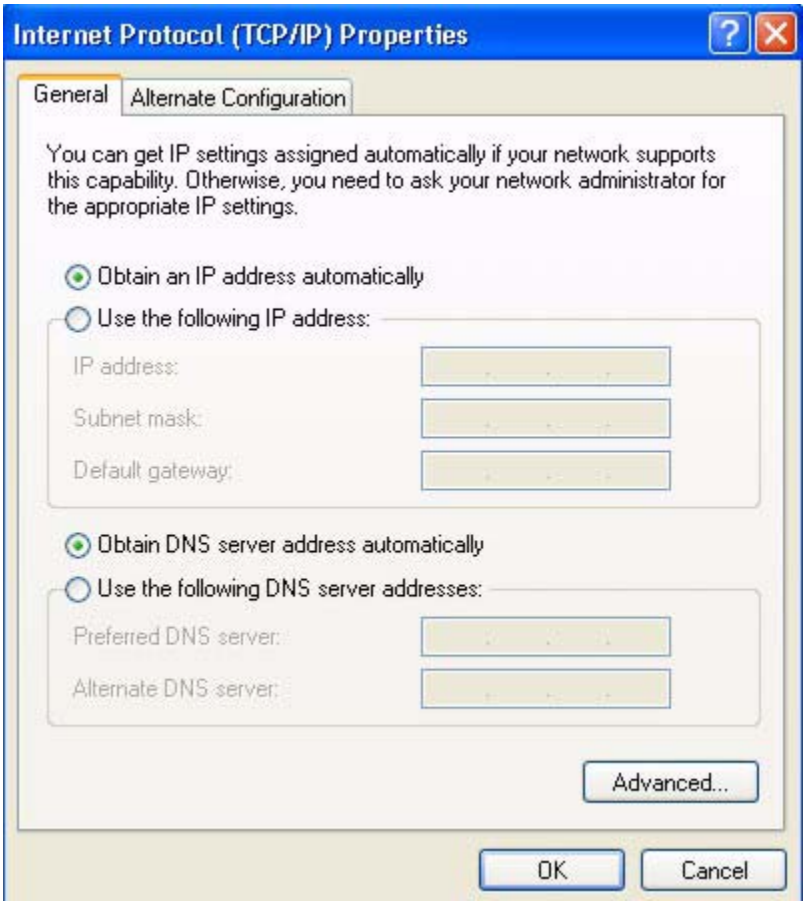
4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

Figure 214 Windows XP: Local Area Connection Properties



5 The **Internet Protocol TCP/IP Properties** window opens.

Figure 215 Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.

7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

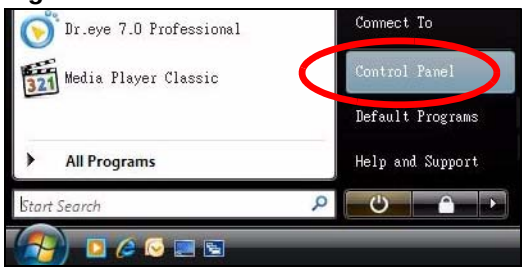
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows Vista

This section shows screens from Windows Vista Professional.

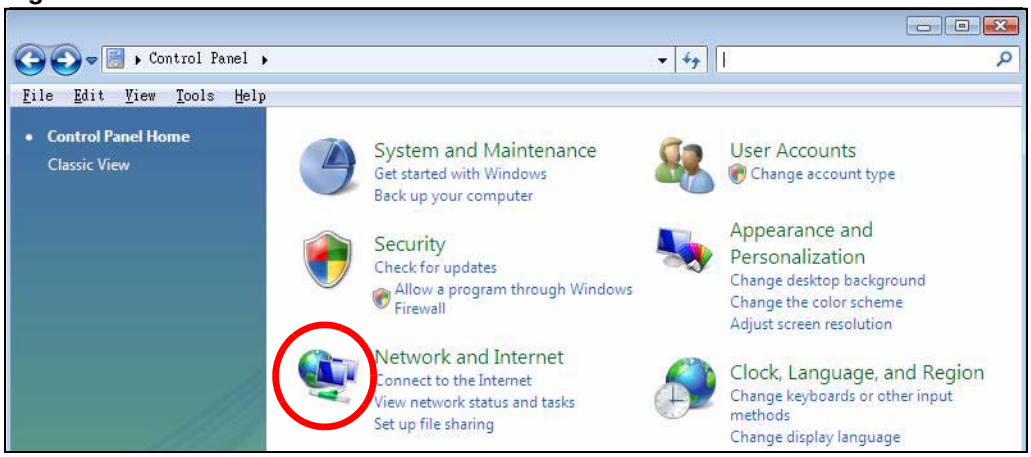
1 Click **Start** > **Control Panel**.

Figure 216 Windows Vista: Start Menu



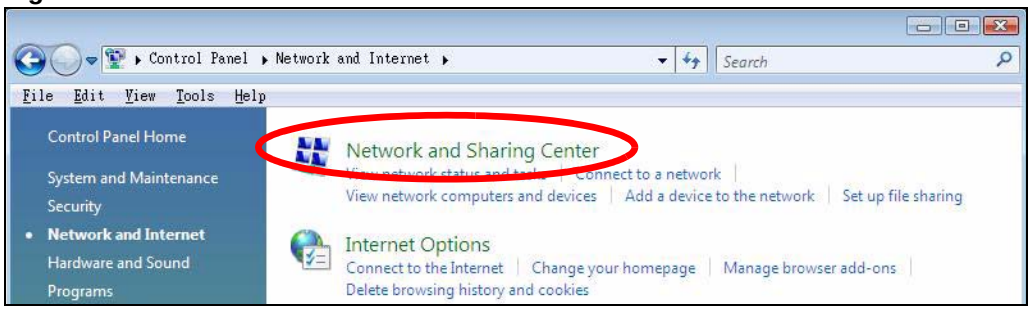
2 In the **Control Panel**, click the **Network and Internet** icon.

Figure 217 Windows Vista: Control Panel



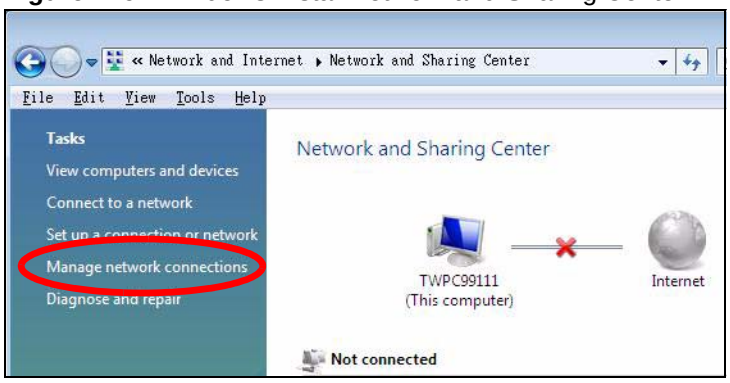
3 Click the **Network and Sharing Center** icon.

Figure 218 Windows Vista: Network And Internet



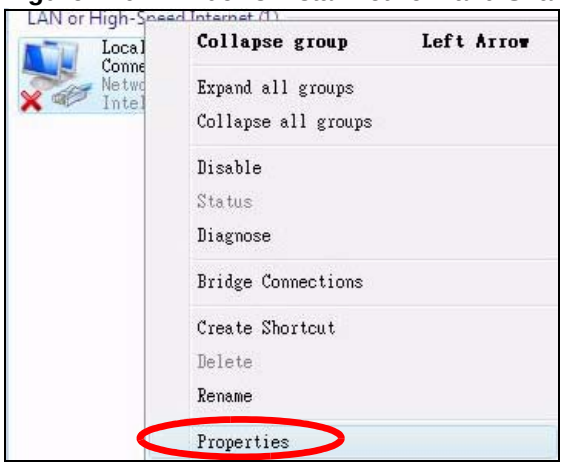
4 Click **Manage network connections**.

Figure 219 Windows Vista: Network and Sharing Center



5 Right-click **Local Area Connection** and then select **Properties**.

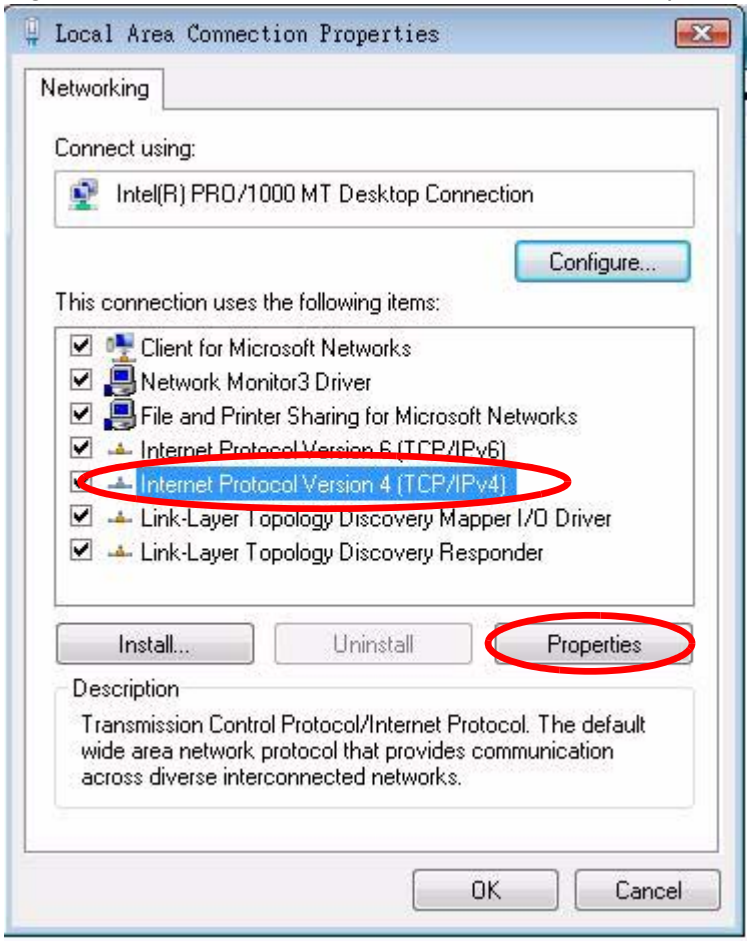
Figure 220 Windows Vista: Network and Sharing Center



During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

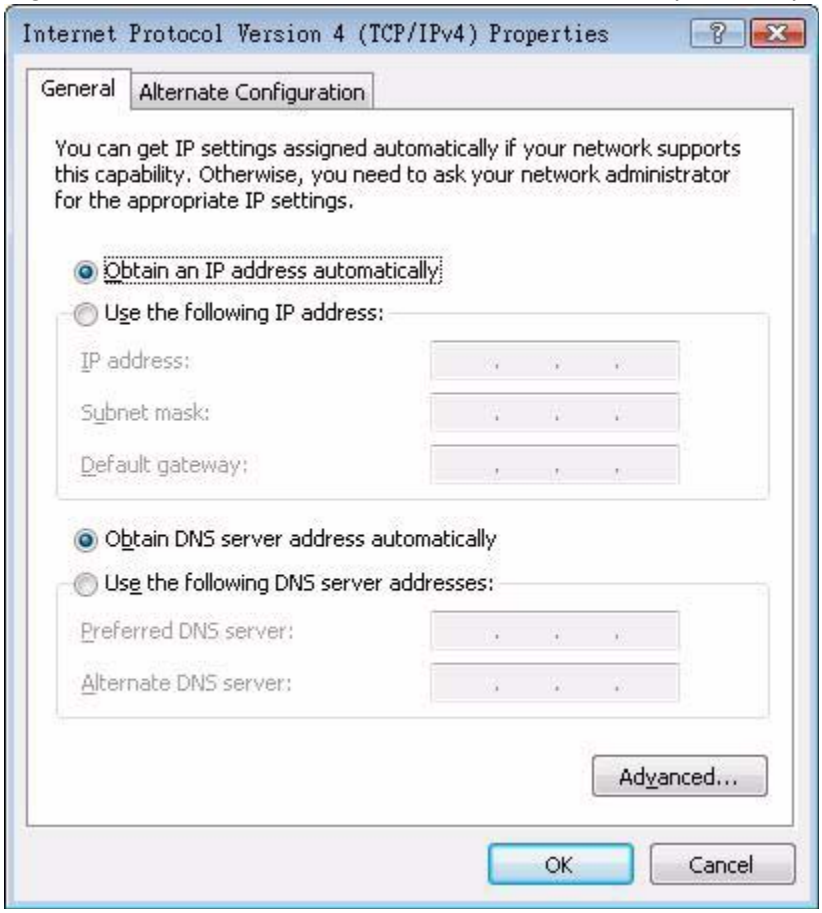
6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 221 Windows Vista: Local Area Connection Properties



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 222 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.Click **Advanced**.

9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

10 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

1 Click **Apple** > **System Preferences**.

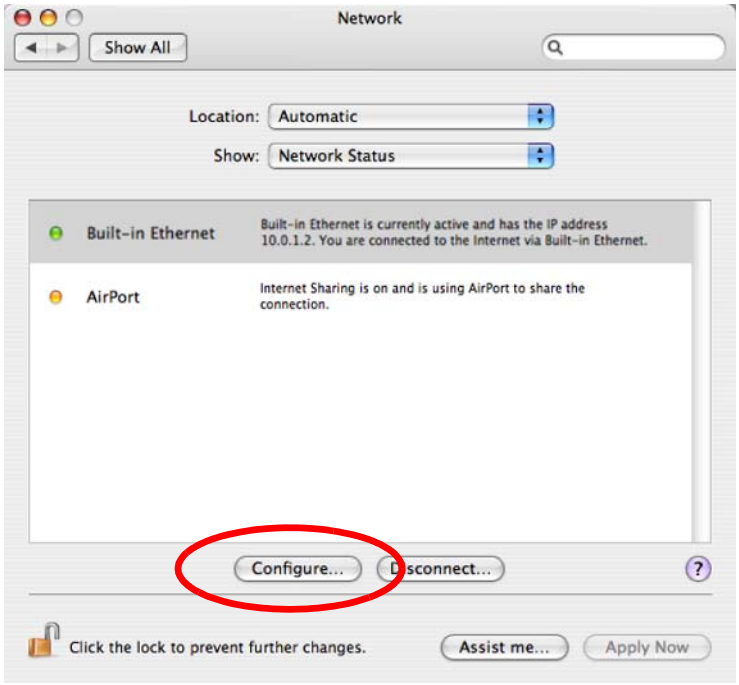
Figure 223 Mac OS X 10.4: Apple Menu

2 In the **System Preferences** window, click the **Network** icon.

Figure 224 Mac OS X 10.4: System Preferences

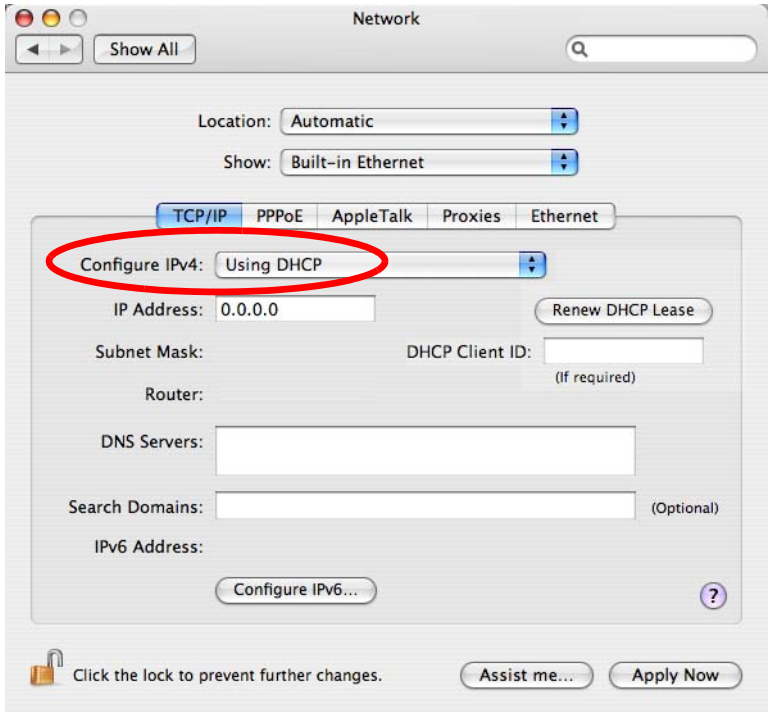
3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure.**

Figure 225 Mac OS X 10.4: Network Preferences


Network
Show All
Location: Automatic
Show: Network Status
Built-in Ethernet
Built-in Ethernet is currently active and has the IP address 10.0.1.2. You are connected to the Internet via Built-in Ethernet.
AirPort
Internet Sharing is on and is using AirPort to share the connection.
Configure...
Disconnect...
Click the lock to prevent further changes.
Assist me...
Apply Now

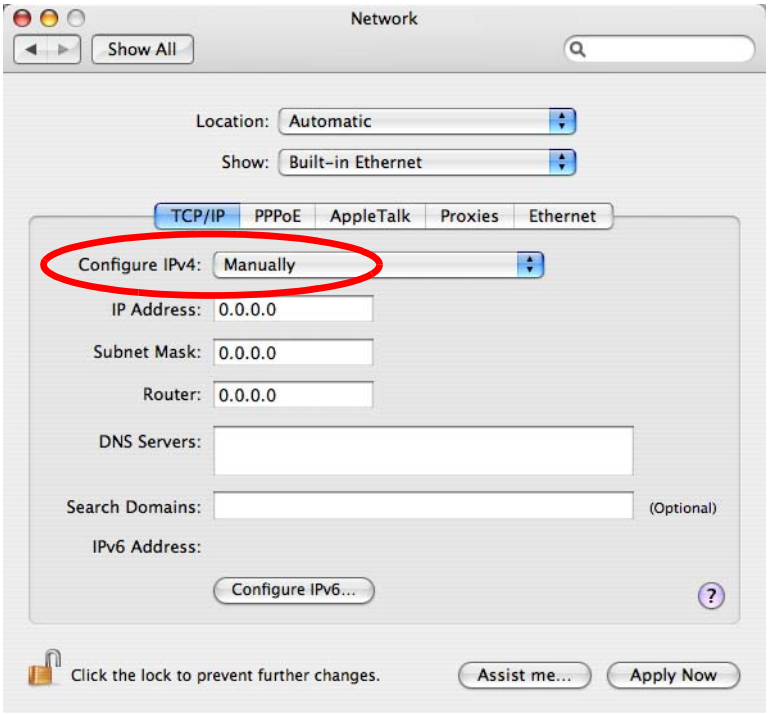
4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.

Figure 226 Mac OS X 10.4: Network Preferences > TCP/IP Tab.



5 For statically assigned settings, do the following:
- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.
- In the **Router** field, type the IP address of your device.

Figure 227 Mac OS X 10.4: Network Preferences > Ethernet

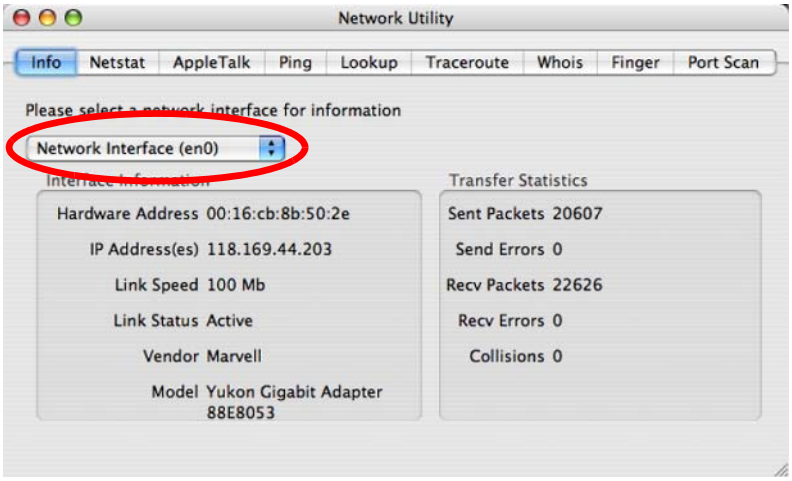


6 Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications** > **Utilities** > **Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

Figure 228 Mac OS X 10.4: Network Utility

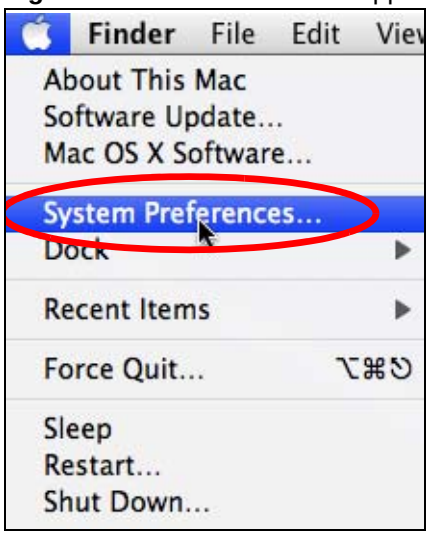


Mac OS X: 10.5

The screens in this section are from Mac OS X 10.5.

1 Click **Apple** > **System Preferences**.

Figure 229 Mac OS X 10.5: Apple Menu

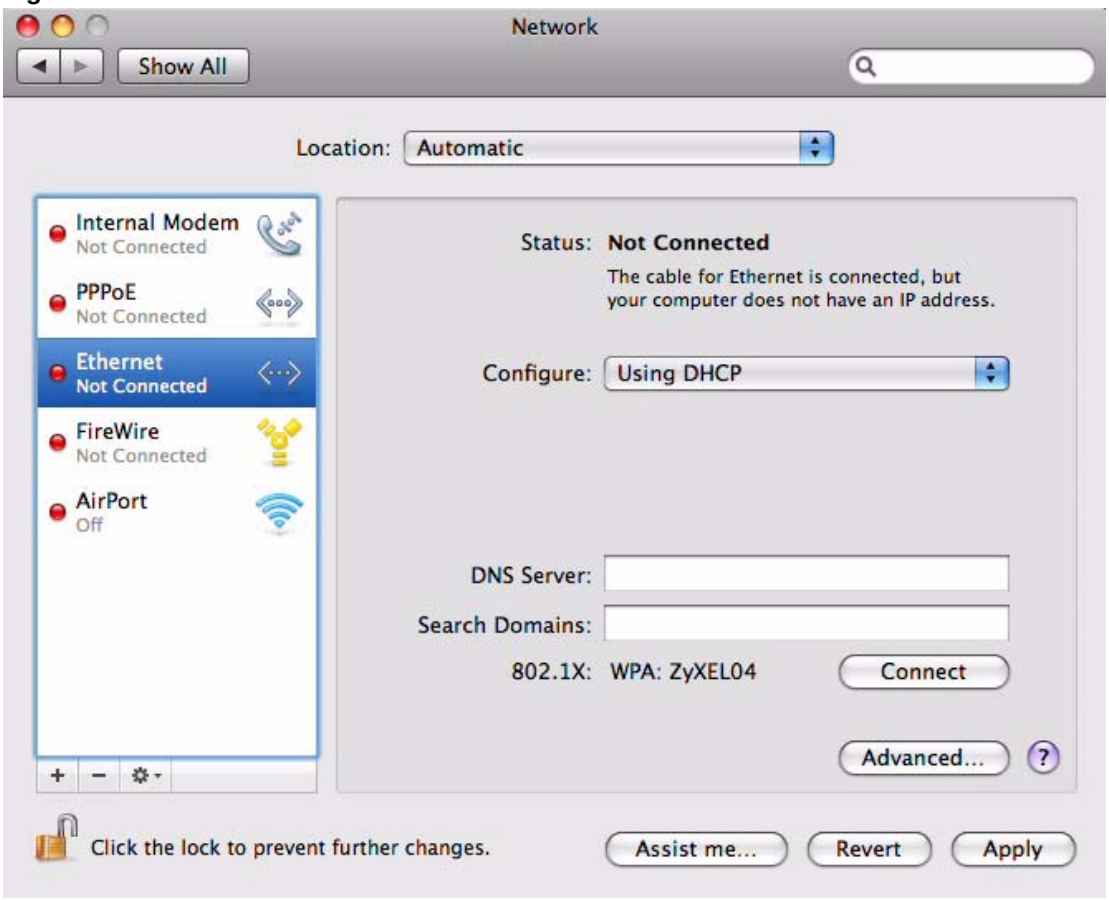


2 In **System Preferences**, click the **Network** icon.

Figure 230 Mac OS X 10.5: Systems Preferences

3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.

Figure 231 Mac OS X 10.5: Network Preferences > Ethernet

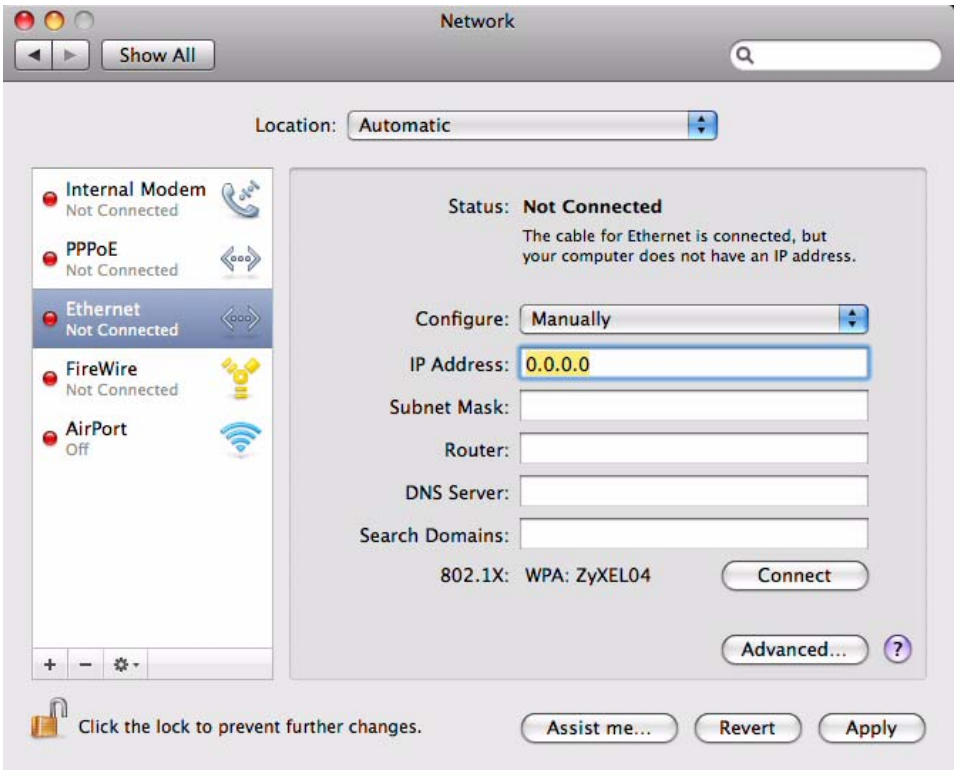


4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.
- In the **Router** field, enter the IP address of your NSA.

Figure 232 Mac OS X 10.5: Network Preferences > Ethernet

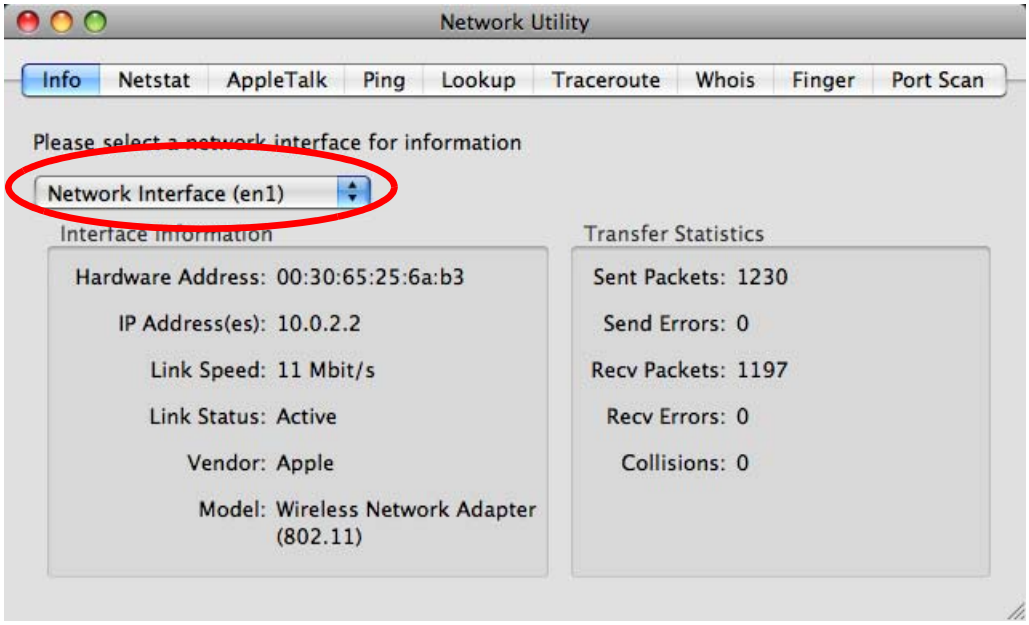


6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications** > **Utilities** > **Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 233 Mac OS X 10.5: Network Utility



Linux: Ubuntu 8 (GNOME)

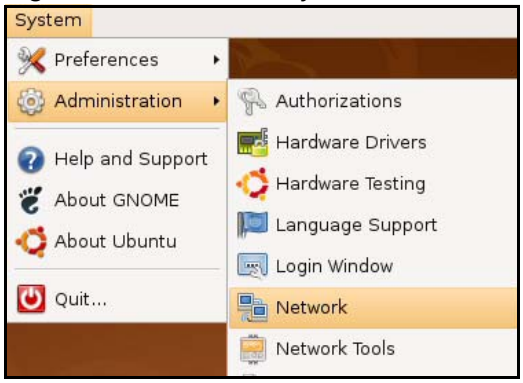
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

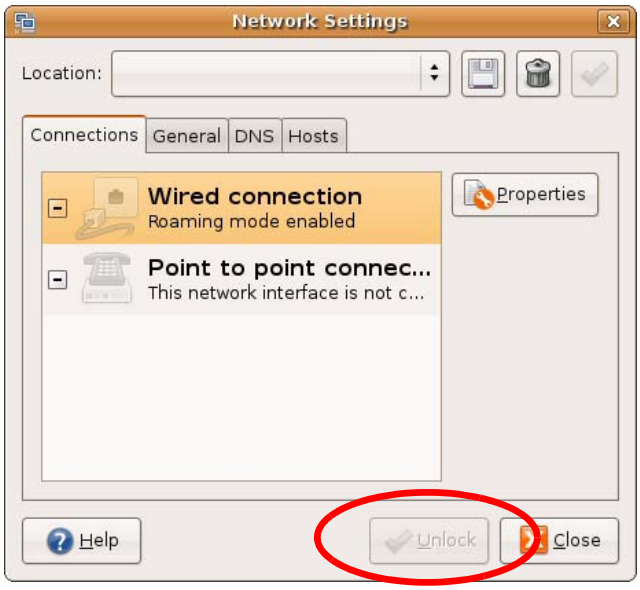
1 Click **System** > **Administration** > **Network**.

Figure 234 Ubuntu 8: System > Administration Menu



2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.

Figure 235 Ubuntu 8: Network Settings > Connections



3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

Figure 236 Ubuntu 8: Administrator Account Authentication

Authenticate
System policy prevents modifying the configuration
An application is attempting to perform an action that requires privileges. Authentication as one of the users below is required to perform this action.
C.J.,,,, (chris)
Password for chris:
Details
Cancel
Authenticate

4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

Figure 237 Ubuntu 8: Network Settings > Connections

5 The **Properties** dialog box opens.

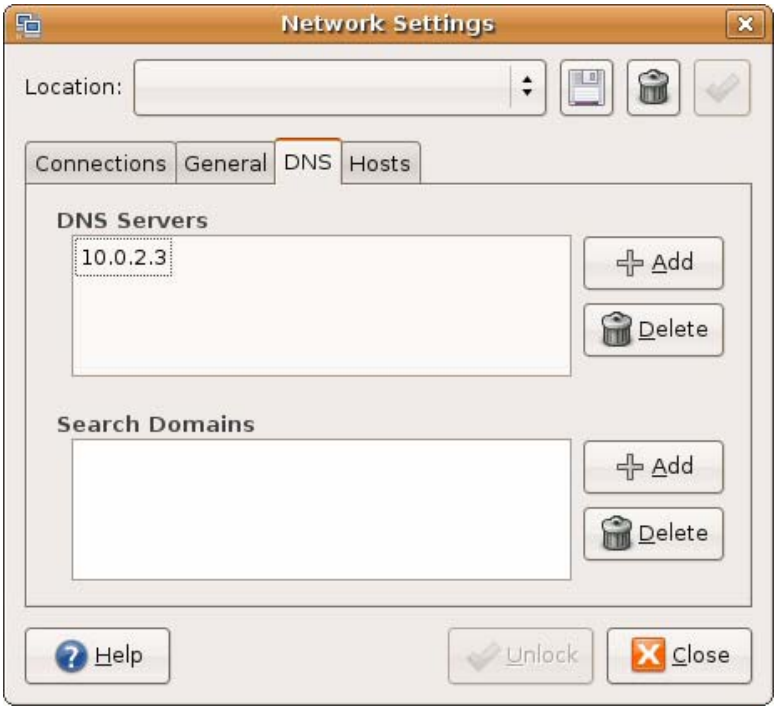
Figure 238 Ubuntu 8: Network Settings > Properties

- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

Figure 239 Ubuntu 8: Network Settings > DNS

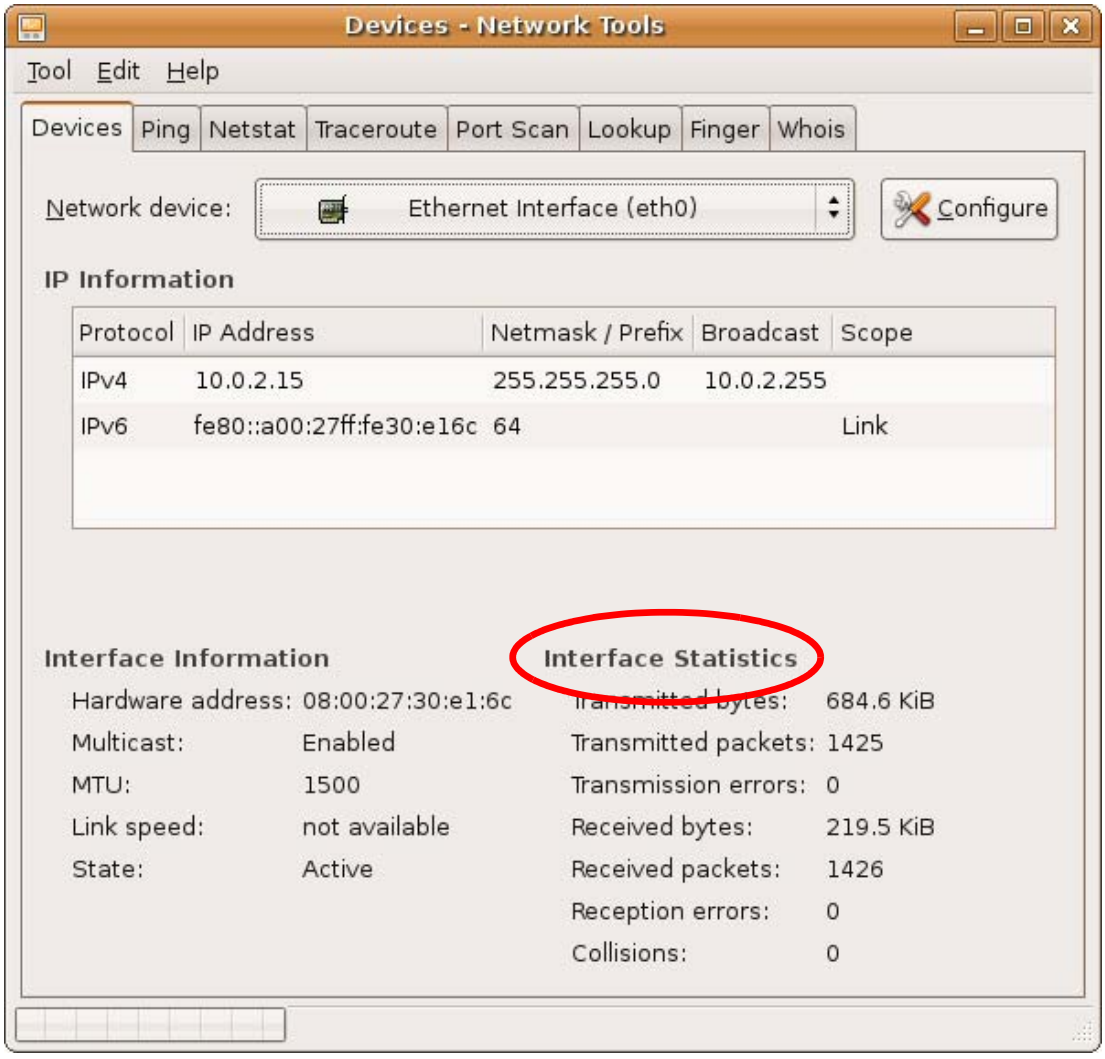


8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices** tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 240 Ubuntu 8: Network Tools



Linux: openSUSE 10.3 (KDE)

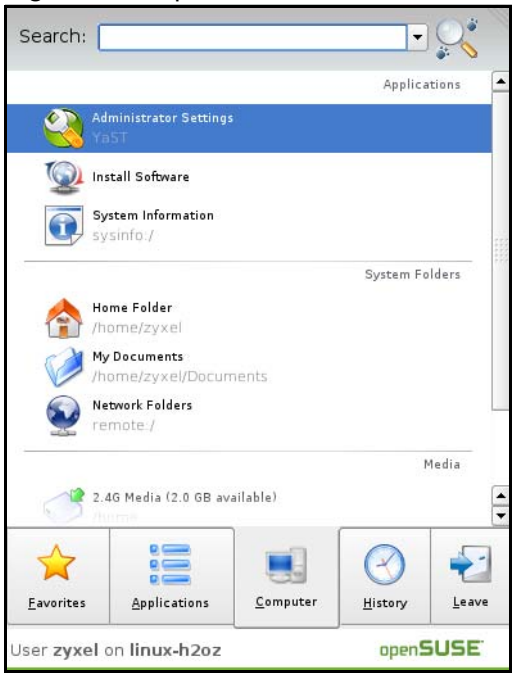
This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in the KDE:

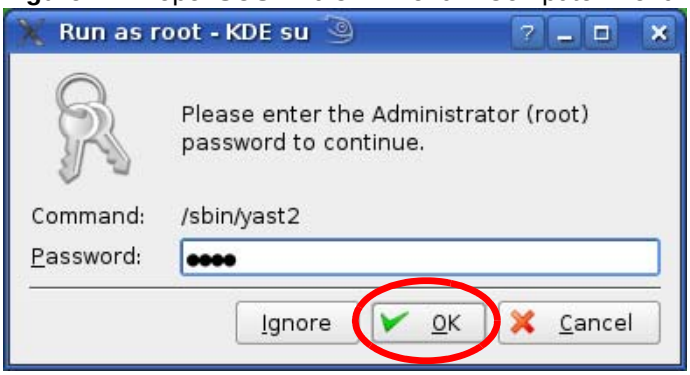
1 Click **K Menu** > **Computer** > **Administrator Settings (YaST)**.

Figure 241 openSUSE 10.3: K Menu > Computer Menu



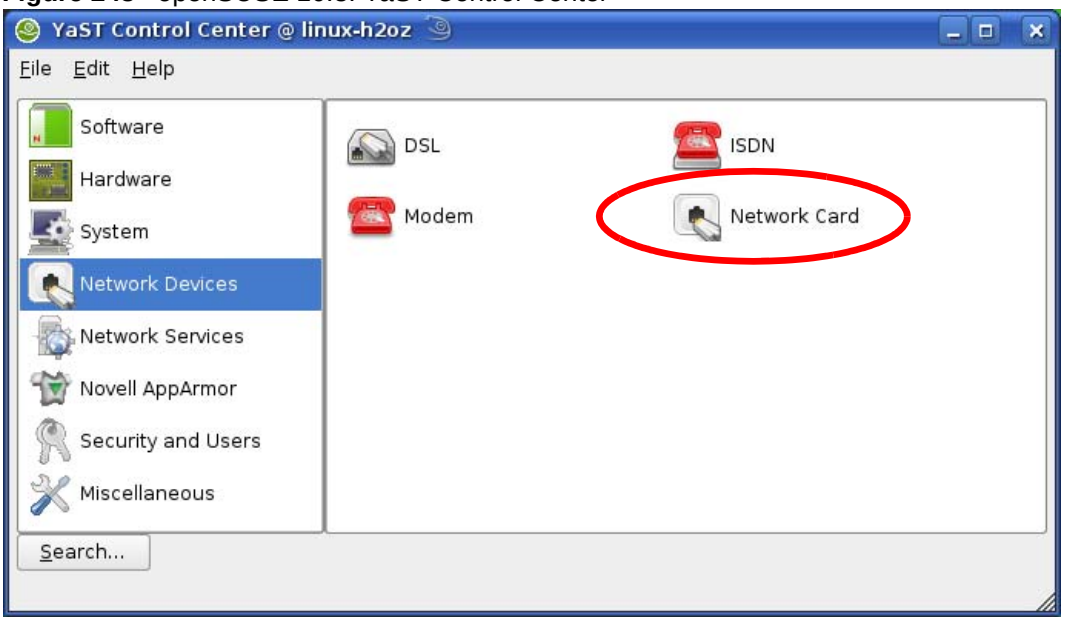
2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

Figure 242 openSUSE 10.3: K Menu > Computer Menu



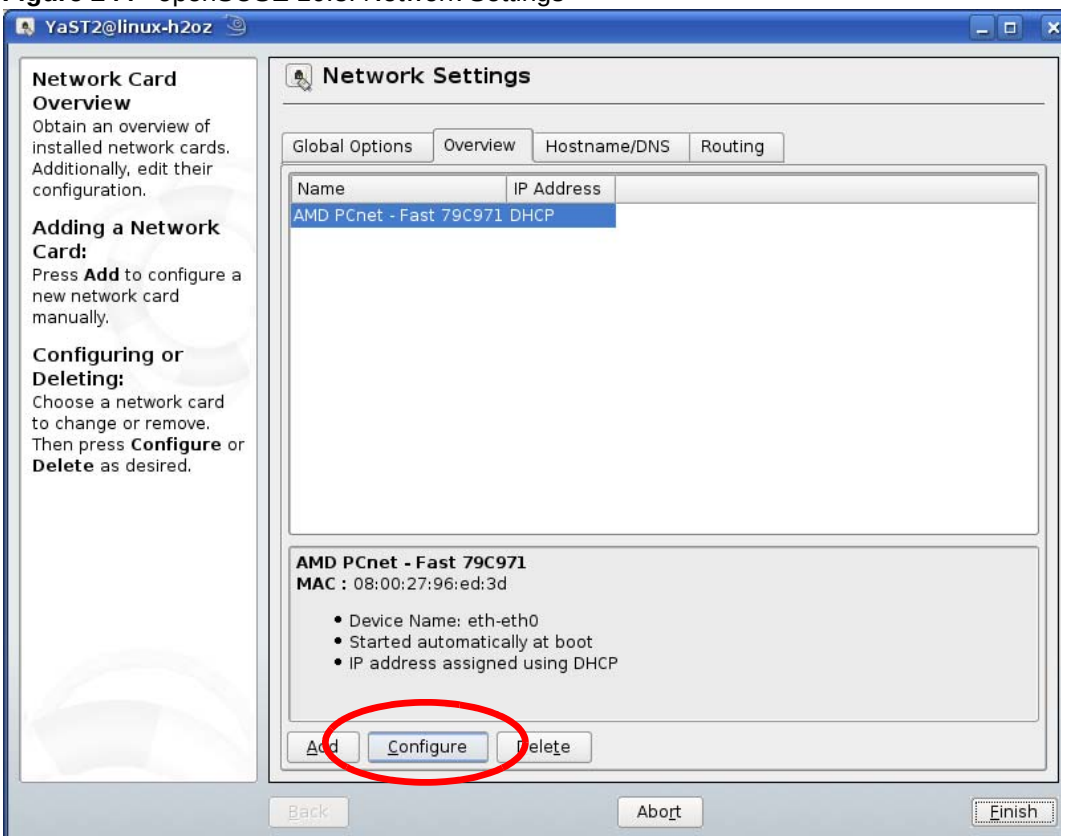
3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

Figure 243 openSUSE 10.3: YaST Control Center



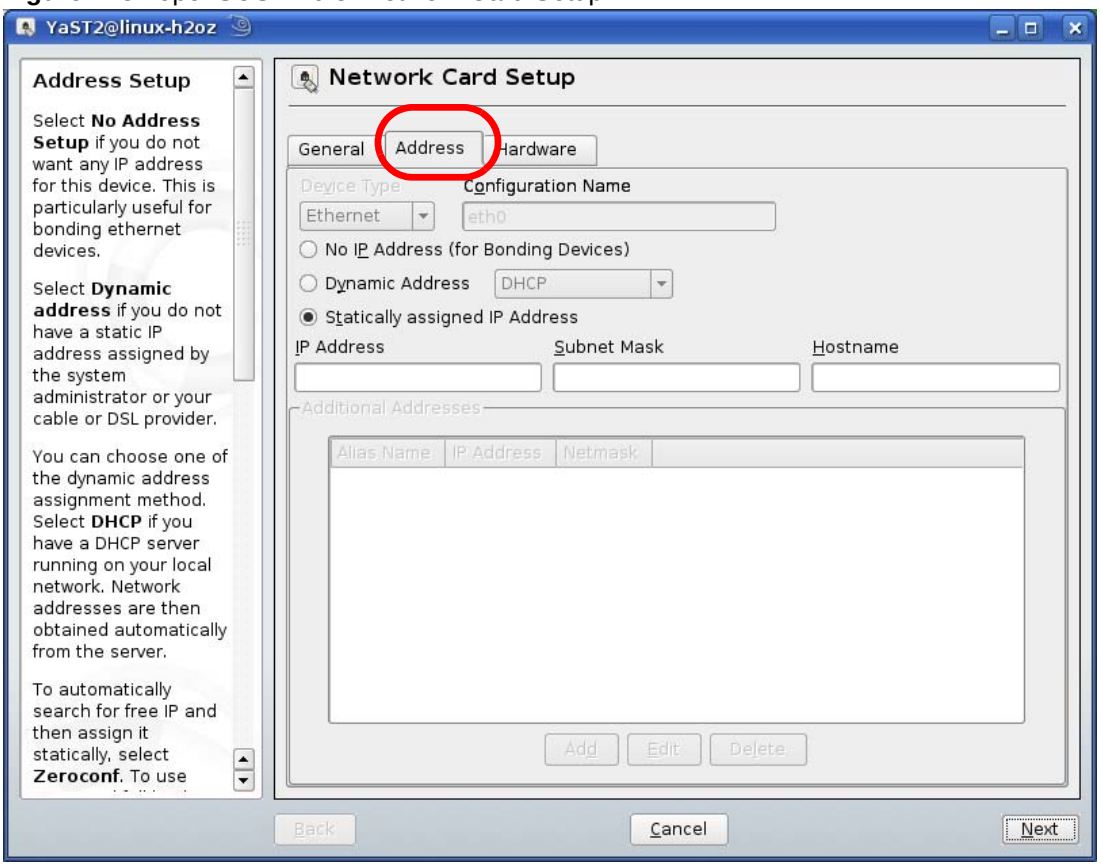
4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

Figure 244 openSUSE 10.3: Network Settings



5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 245 openSUSE 10.3: Network Card Setup

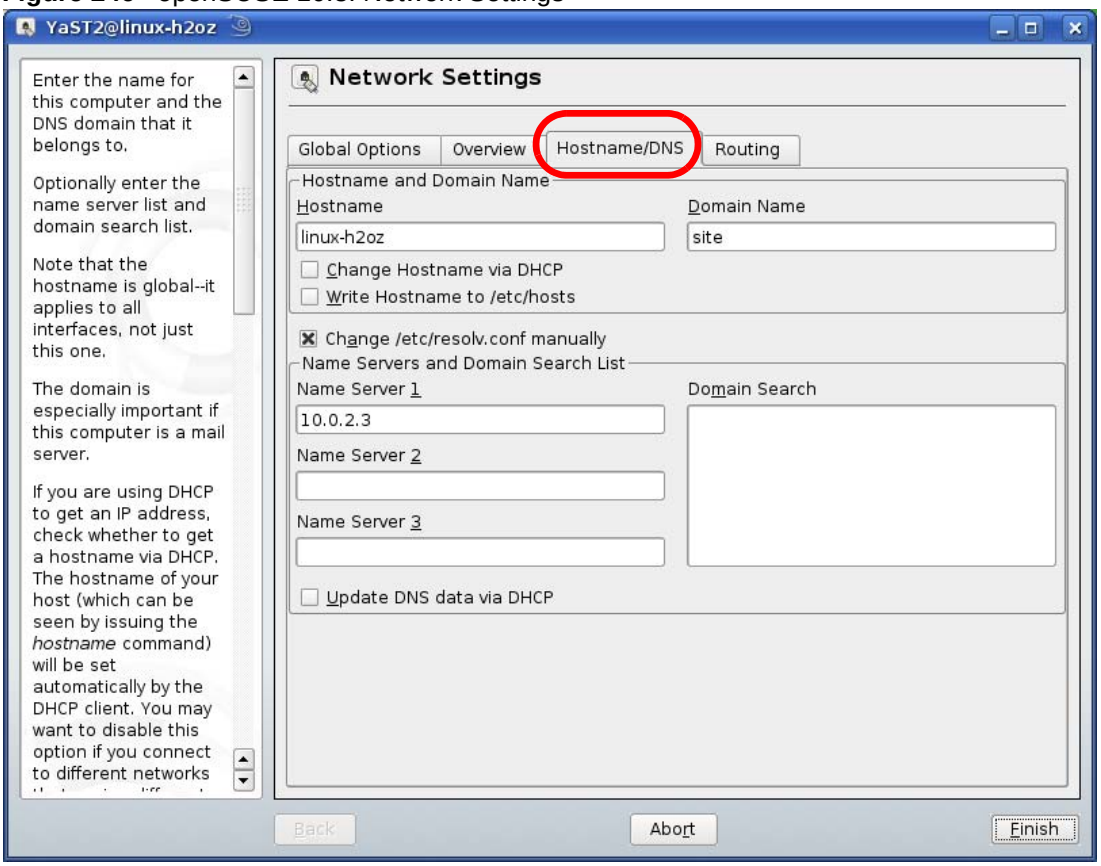

YaST2@linux-h2oz
Address Setup
Select No Address Setup if you do not want any IP address for this device. This is particularly useful for bonding ethernet devices.
Select Dynamic address if you do not have a static IP address assigned by the system administrator or your cable or DSL provider.
You can choose one of the dynamic address assignment method. Select DHCP if you have a DHCP server running on your local network. Network addresses are then obtained automatically from the server.
To automatically search for free IP and then assign it statically, select Zeroconf. To use
Network Card Setup
General
Address
Hardware
Device Type
Configuration Name
Ethernet
eth0
No IP Address (for Bonding Devices)
Dynamic Address
DHCP
Statically assigned IP Address
IP Address
Subnet Mask
Hostname
Additional Addresses
Alias Name
IP Address
Netmask
Add
Edit
Delete
Back
Cancel
Next

6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.
Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7 Click **Next** to save the changes and close the **Network Card Setup** window.

8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

Figure 246 openSUSE 10.3: Network Settings

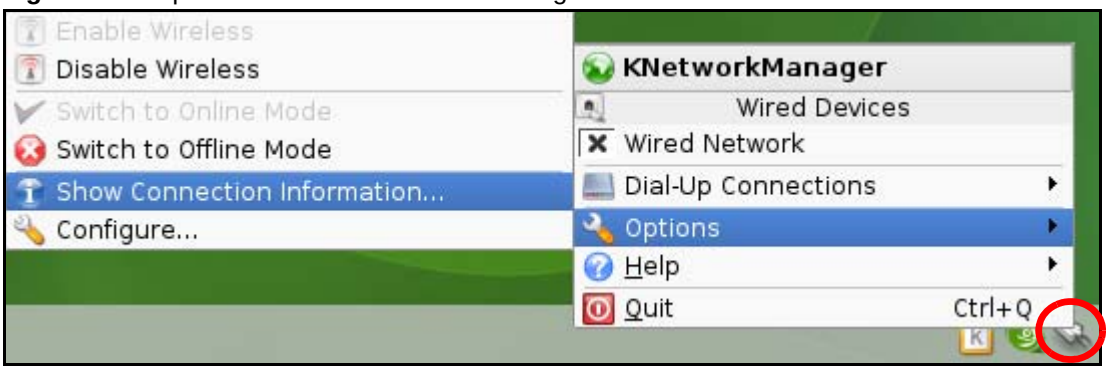

YaST2@linux-h2oz
Enter the name for this computer and the DNS domain that it belongs to.
Optionally enter the name server list and domain search list.
Note that the hostname is global--it applies to all interfaces, not just this one.
The domain is especially important if this computer is a mail server.
If you are using DHCP to get an IP address, check whether to get a hostname via DHCP. The hostname of your host (which can be seen by issuing the hostname command) will be set automatically by the DHCP client. You may want to disable this option if you connect to different networks
Network Settings
Global Options
Overview
Hostname/DNS
Routing
Hostname and Domain Name
Hostname
linux-h2oz
Domain Name
site
Change Hostname via DHCP
Write Hostname to /etc/hosts
Change /etc/resolv.conf manually
Name Servers and Domain Search List
Name Server 1
10.0.2.3
Domain Search
Name Server 2
Name Server 3
Update DNS data via DHCP
Back
Abort
Finish

9 Click **Finish** to save your settings and close the window.

Verifying Settings

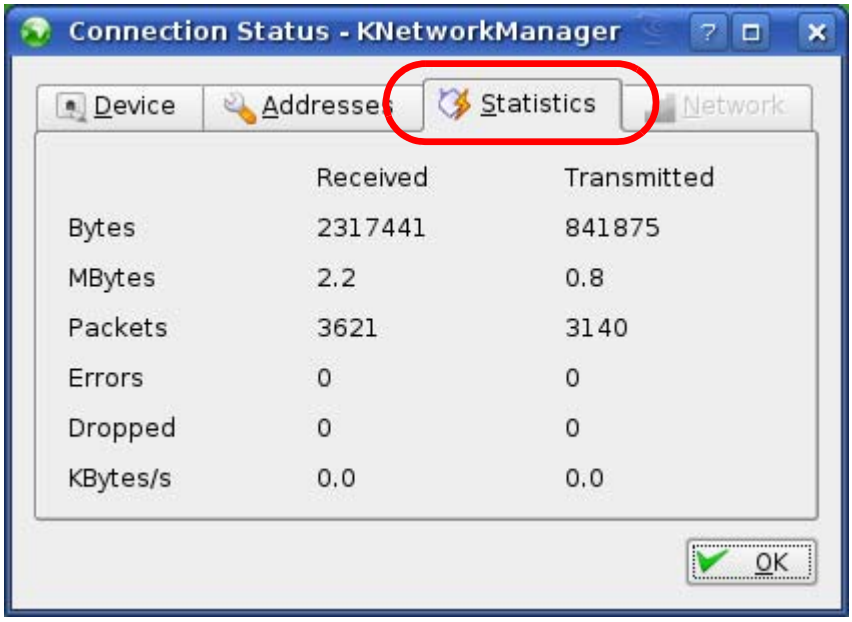
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 247 openSUSE 10.3: KNetwork Manager



When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

Figure 248 openSUSE: Connection Status - KNetwork Manager



C

Importing Certificates

This appendix shows you how to import public key certificates into your web browser.

Public key certificates are used by web browsers to ensure that a secure web site is legitimate. When a certificate authority such as VeriSign, Comodo, or Network Solutions, to name a few, receives a certificate request from a website operator, they confirm that the web domain and contact information in the request match those on public record with a domain name registrar. If they match, then the certificate is issued to the website operator, who then places it on the site to be issued to all visiting web browsers to let them know that the site is legitimate.

Many ZyXEL products, such as the NSA-2401, issue their own public key certificates. These can be used by web browsers on a LAN or WAN to verify that they are in fact connecting to the legitimate device and not one masquerading as it. However, because the certificates were not issued by one of the several organizations officially recognized by the most common web browsers, you will need to import the ZyXEL-created certificate into your web browser and flag that certificate as a trusted authority.

You can see if you are browsing on a secure website if the URL in your web browser's address bar begins with `https://` or there is a sealed padlock icon ( ) somewhere in the main browser window (not all browsers show the padlock in the same location.)

In this appendix, you can import a public key certificate for:

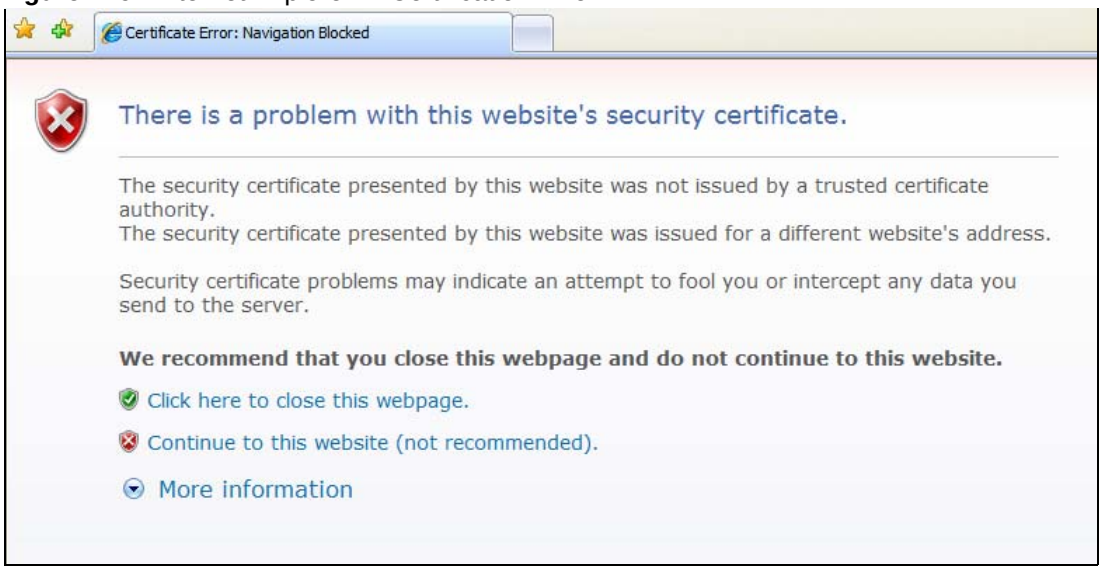
- Internet Explorer on page 300
- Firefox on page 308
- Opera on page 313
- Konqueror on page 319

Internet Explorer

The following example uses Microsoft Internet Explorer 7 on Windows XP Professional; however, they can also apply to Internet Explorer on Windows Vista.

1 If your device's Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

Figure 249 Internet Explorer 7: Certification Error

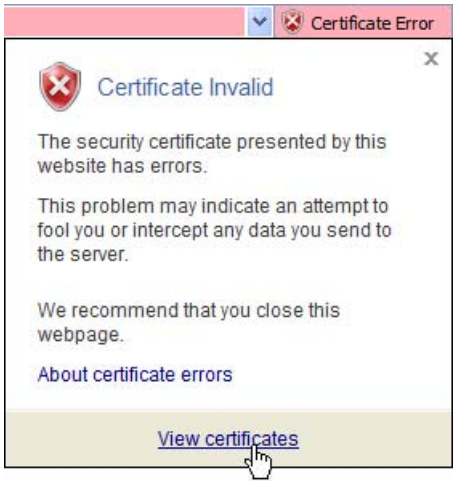

Certificate Error: Navigation Blocked
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

2 Click **Continue to this website (not recommended)**.

Figure 250 Internet Explorer 7: Certification Error

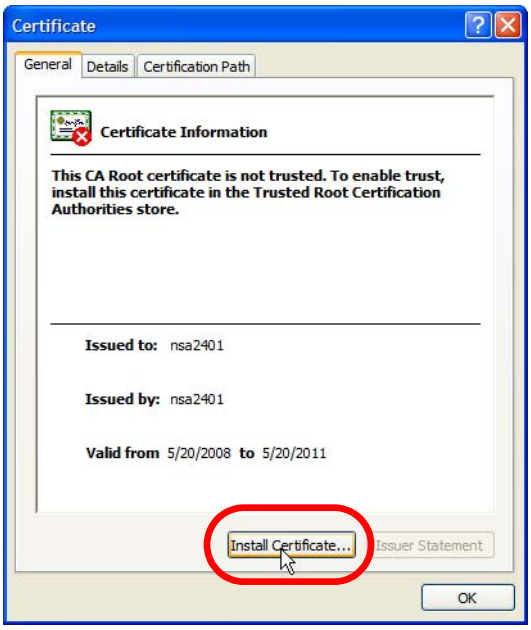
3 In the **Address Bar**, click **Certificate Error** > **View certificates**.

Figure 251 Internet Explorer 7: Certificate Error


Certificate Error
Certificate Invalid
The security certificate presented by this website has errors.
This problem may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage.
About certificate errors
View certificates

4 In the **Certificate** dialog box, click **Install Certificate**.

Figure 252 Internet Explorer 7: Certificate



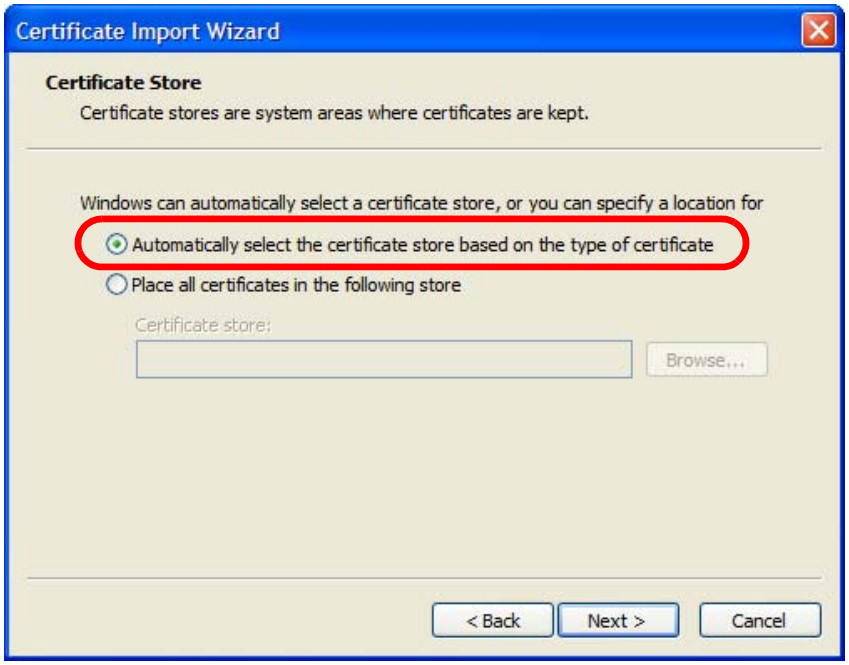
5 In the **Certificate Import Wizard**, click **Next**.

Figure 253 Internet Explorer 7: Certificate Import Wizard

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

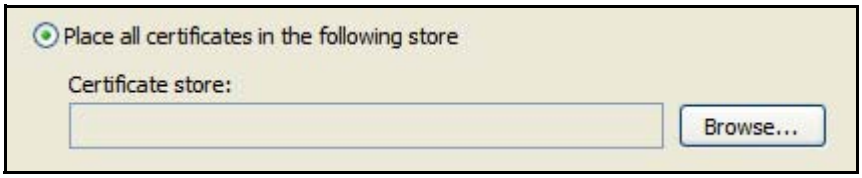
6 If you want Internet Explorer to **Automatically select certificate store based on the type of certificate**, click **Next** again and then go to step 9.

Figure 254 Internet Explorer 7: Certificate Import Wizard


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel

7 Otherwise, select **Place all certificates in the following store** and then click **Browse**.

Figure 255 Internet Explorer 7: Certificate Import Wizard

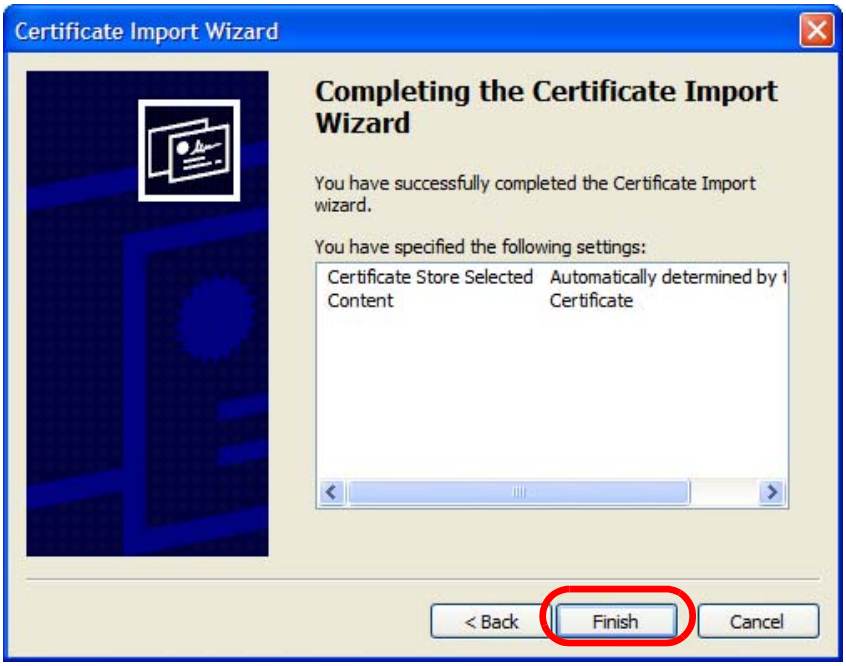


8 In the **Select Certificate Store** dialog box, choose a location in which to save the certificate and then click **OK**.

Figure 256 Internet Explorer 7: Select Certificate Store

9 In the **Completing the Certificate Import Wizard** screen, click **Finish**.

Figure 257 Internet Explorer 7: Certificate Import Wizard



10 If you are presented with another **Security Warning**, click **Yes**.

Figure 258 Internet Explorer 7: Security Warning

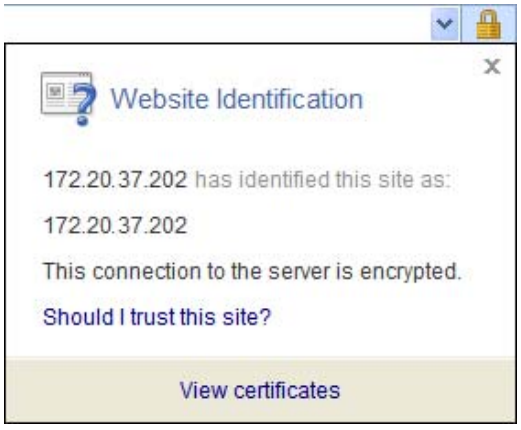
Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
nsa2401
Windows cannot validate that the certificate is actually from "nsa2401". You should confirm its origin by contacting "nsa2401". The following number will assist you in this process:
Thumbprint (sha1): 35D1C9AC DBC0E654 FE327C71 464D154B 242E5B93
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No

11 Finally, click **OK** when presented with the successful certificate installation message.

Figure 259 Internet Explorer 7: Certificate Import Wizard

12 The next time you start Internet Explorer and go to a ZyXEL Web Configurator page, a sealed padlock icon appears in the address bar. Click it to view the page's **Website Identification** information.

Figure 260 Internet Explorer 7: Website Identification



Installing a Stand-Alone Certificate File in Internet Explorer

Rather than browsing to a ZyXEL Web Configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

1 Double-click the public key certificate file.

Figure 261 Internet Explorer 7: Public Key Certificate File

2 In the security warning dialog box, click **Open**.

Figure 262 Internet Explorer 7: Open File - Security Warning

Open File - Security Warning
Do you want to open this file?
Name: CA.cer
Publisher: Unknown Publisher
Type: Security Certificate
From: D:\Documents and Settings\13435\Desktop
Open
Cancel
Always ask before opening this file
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

3 Refer to steps 4-12 in the Internet Explorer procedure beginning on page 300 to complete the installation process.

Removing a Certificate in Internet Explorer

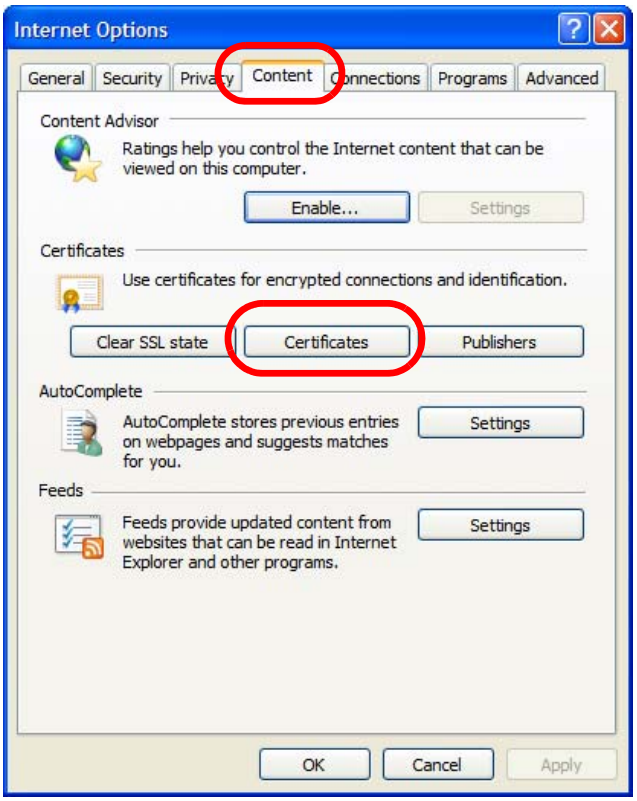
This section shows you how to remove a public key certificate in Internet Explorer 7.

1 Open **Internet Explorer** and click **Tools** > **Internet Options**.

Figure 263 Internet Explorer 7: Tools Menu

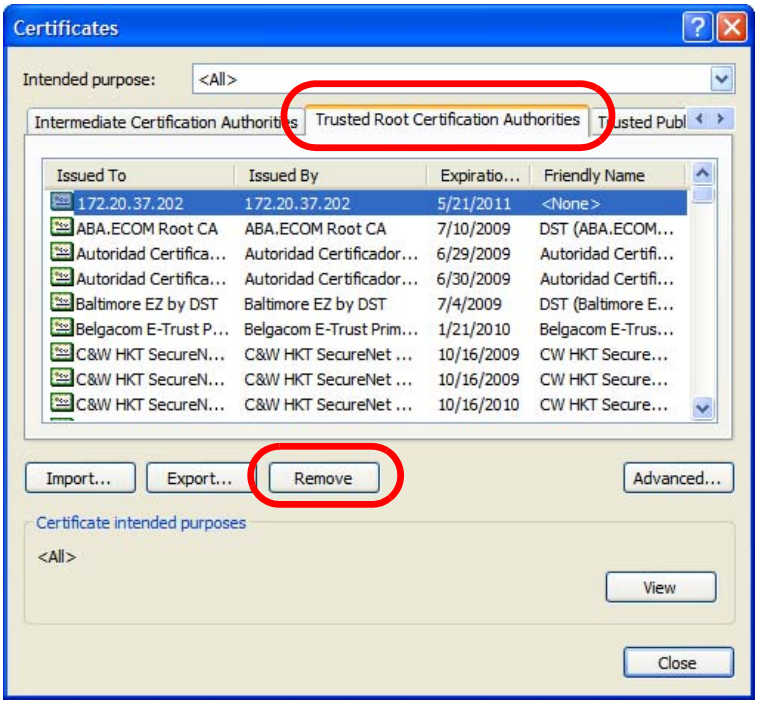
2 In the **Internet Options** dialog box, click **Content** > **Certificates**.

Figure 264 Internet Explorer 7: Internet Options



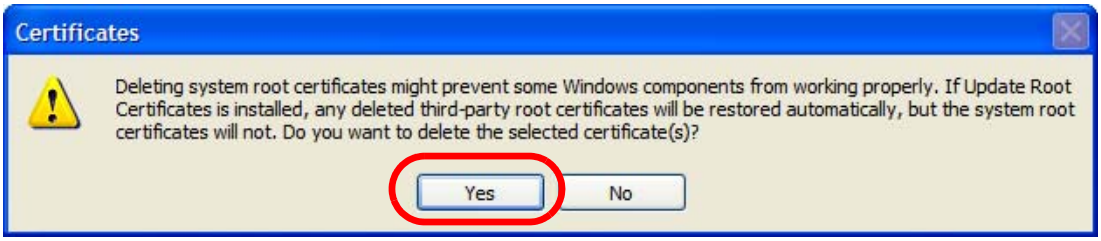
3 In the **Certificates** dialog box, click the **Trusted Root Certificates Authorities** tab, select the certificate that you want to delete, and then click **Remove**.

Figure 265 Internet Explorer 7: Certificates



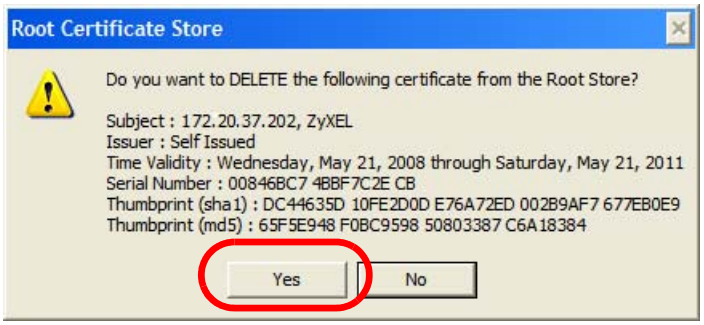
4 In the **Certificates** confirmation, click **Yes**.

Figure 266 Internet Explorer 7: Certificates


Certificates
Deleting system root certificates might prevent some Windows components from working properly. If Update Root Certificates is installed, any deleted third-party root certificates will be restored automatically, but the system root certificates will not. Do you want to delete the selected certificate(s)?
Yes
No

5 In the **Root Certificate Store** dialog box, click **Yes**.

Figure 267 Internet Explorer 7: Root Certificate Store


Root Certificate Store
Do you want to DELETE the following certificate from the Root Store?
Subject : 172.20.37.202, ZyXEL
Issuer : Self Issued
Time Validity : Wednesday, May 21, 2008 through Saturday, May 21, 2011
Serial Number : 00846BC7 4BBF7C2E CB
Thumbprint (sha1) : DC44635D 10FE2D0D E76A72ED 002B9AF7 677EB0E9
Thumbprint (md5) : 65F5E948 F0BC9598 50803387 C6A18384
Yes
No

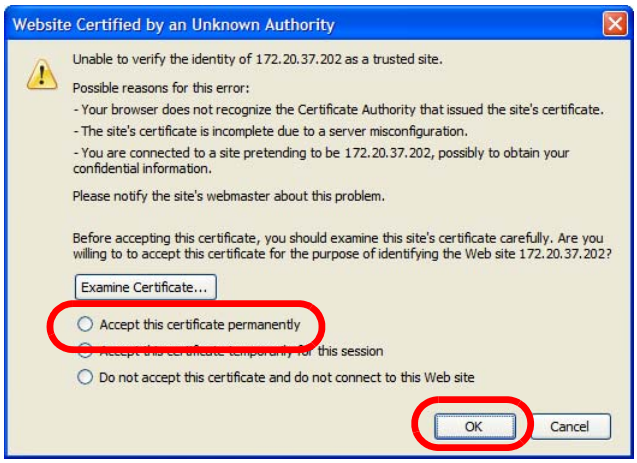
6 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

Firefox

The following example uses Mozilla Firefox 2 on Windows XP Professional; however, the screens can also apply to Firefox 2 on all platforms.

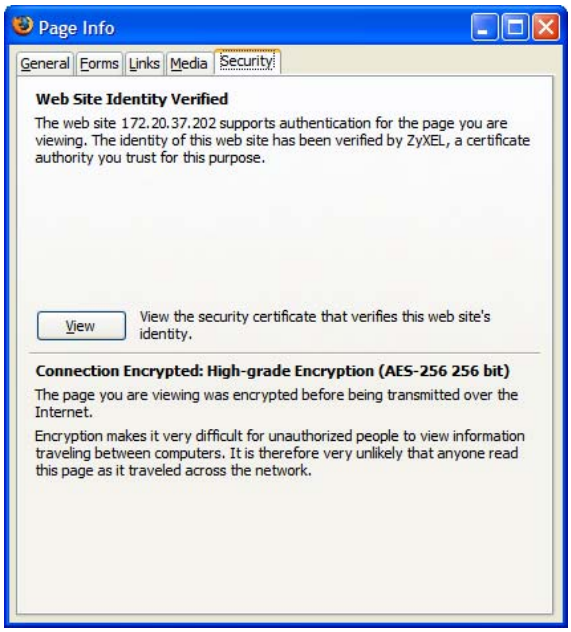
1. If your device's Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
2. Select **Accept this certificate permanently** and click **OK.**

Figure 268 Firefox 2: Website Certified by an Unknown Authority


Website Certified by an Unknown Authority
Unable to verify the identity of 172.20.37.202 as a trusted site.
Possible reasons for this error:
- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be 172.20.37.202, possibly to obtain your confidential information.
Please notify the site's webmaster about this problem.
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site 172.20.37.202?
Examine Certificate...
Accept this certificate permanently
Do not accept this certificate and do not connect to this Web site
OK
Cancel

3. The certificate is stored and you can now connect securely to the Web Configurator. A sealed padlock appears in the address bar, which you can click to open the **Page Info** > **Security** window to view the web page's security information.

Figure 269 Firefox 2: Page Info

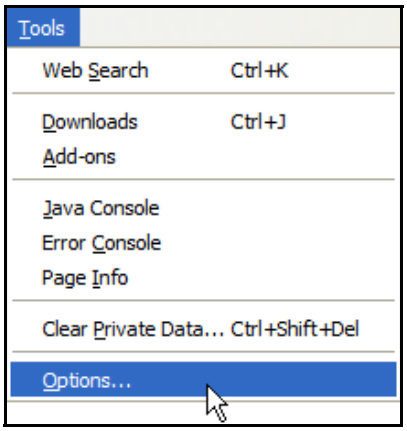

Page Info
General
Forms
Links
Media
Security
Web Site Identity Verified
The web site 172.20.37.202 supports authentication for the page you are viewing. The identity of this web site has been verified by ZyXEL, a certificate authority you trust for this purpose.
View
View the security certificate that verifies this web site's identity.
Connection Encrypted: High-grade Encryption (AES-256 256 bit)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

Installing a Stand-Alone Certificate File in Firefox

Rather than browsing to a ZyXEL Web Configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

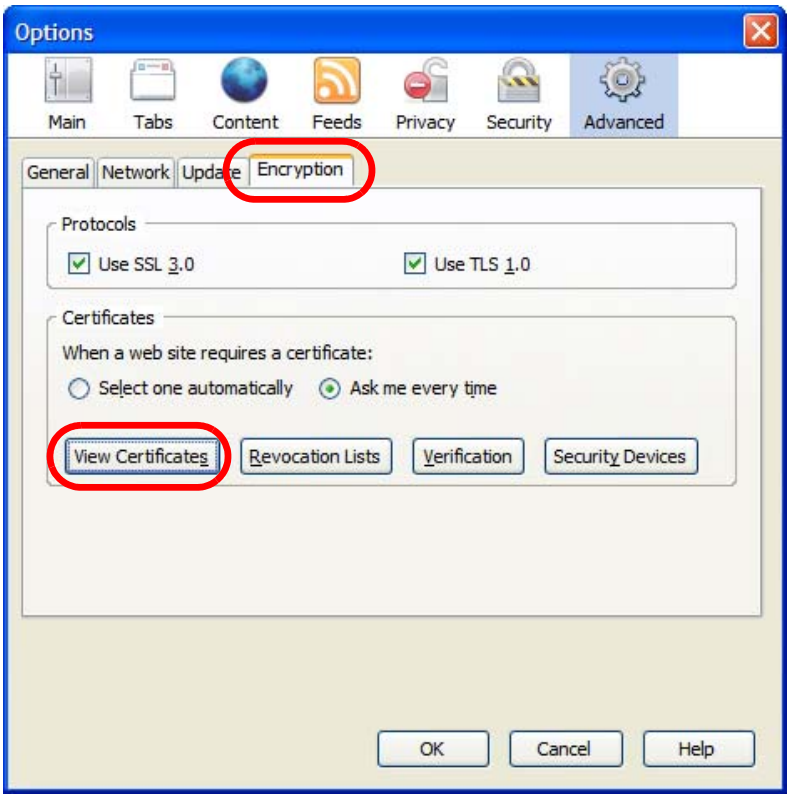
1 Open **Firefox** and click **Tools** > **Options**.

Figure 270 Firefox 2: Tools Menu



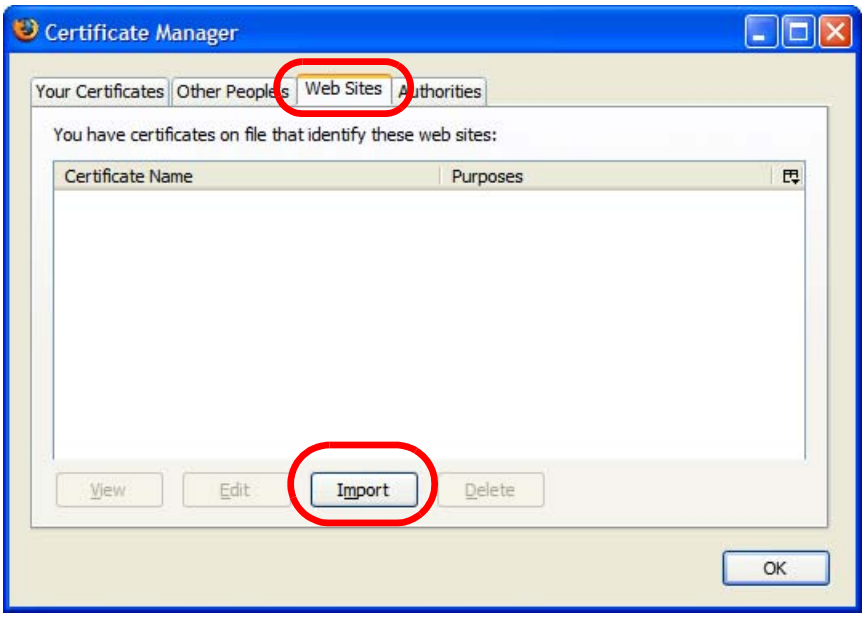
2 In the **Options** dialog box, click **Advanced** > **Encryption** > **View Certificates**.

Figure 271 Firefox 2: Options



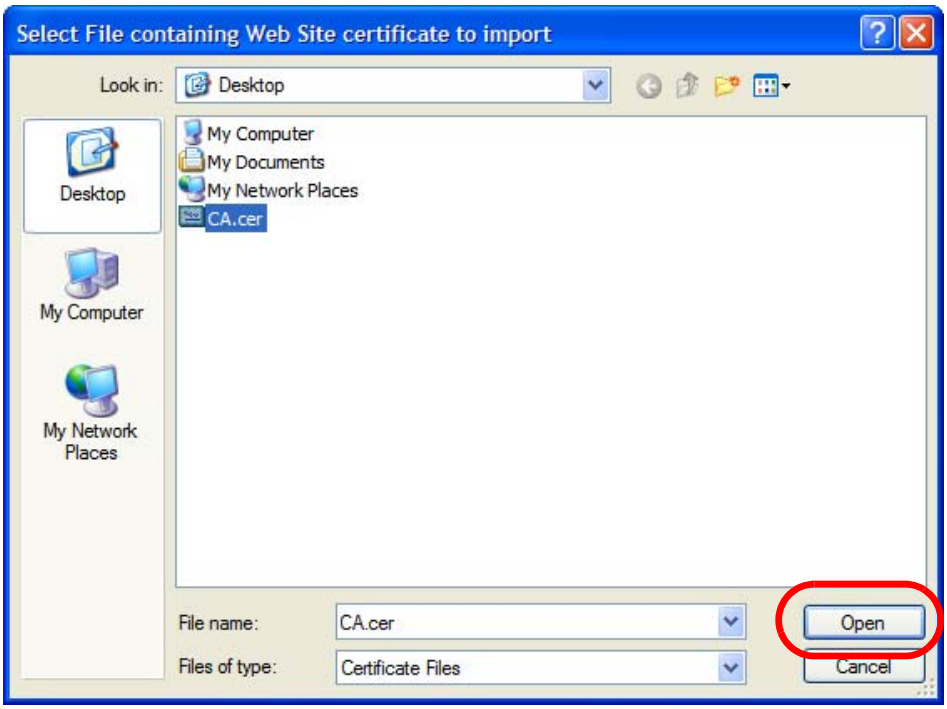
3 In the **Certificate Manager** dialog box, click **Web Sites** > **Import**.

Figure 272 Firefox 2: Certificate Manager



4 Use the **Select File** dialog box to locate the certificate and then click **Open**.

Figure 273 Firefox 2: Select File



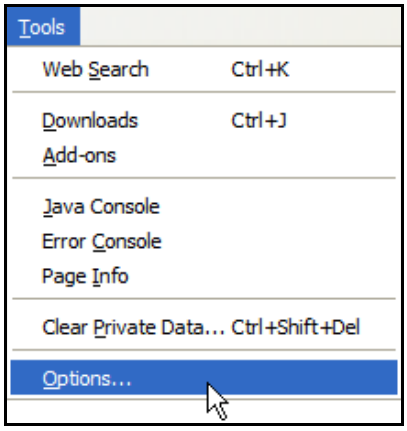
5 The next time you visit the web site, click the padlock in the address bar to open the **Page Info** > **Security** window to see the web page's security information.

Removing a Certificate in Firefox

This section shows you how to remove a public key certificate in Firefox 2.

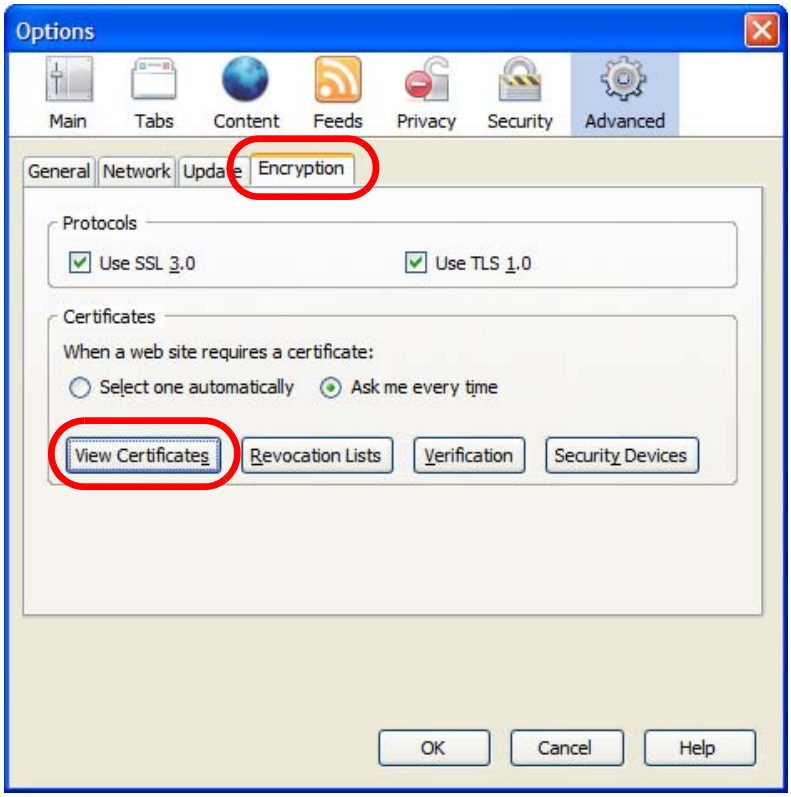
1 Open **Firefox** and click **Tools** > **Options**.

Figure 274 Firefox 2: Tools Menu



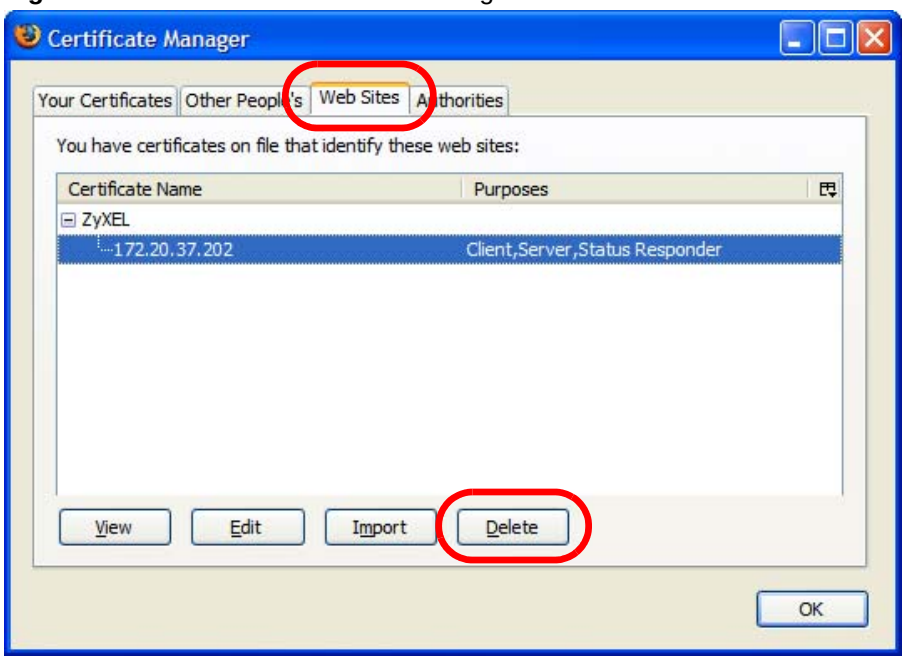
2 In the **Options** dialog box, click **Advanced** > **Encryption** > **View Certificates**.

Figure 275 Firefox 2: Options



3 In the **Certificate Manager** dialog box, select the **Web Sites** tab, select the certificate that you want to remove, and then click **Delete**.

Figure 276 Firefox 2: Certificate Manager



4 In the **Delete Web Site Certificates** dialog box, click **OK**.

Figure 277 Firefox 2: Delete Web Site Certificates

Delete Web Site Certificates
Are you sure you want to delete these web site certificates?
172.20.37.202
If you delete a web site certificate, you will be asked to accept it again the next time you visit the web site.
OK
Cancel

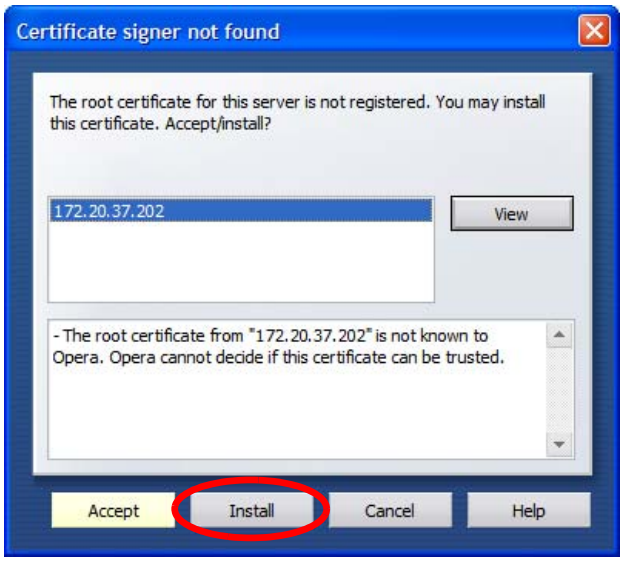
5 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

Opera

The following example uses Opera 9 on Windows XP Professional; however, the screens can apply to Opera 9 on all platforms.

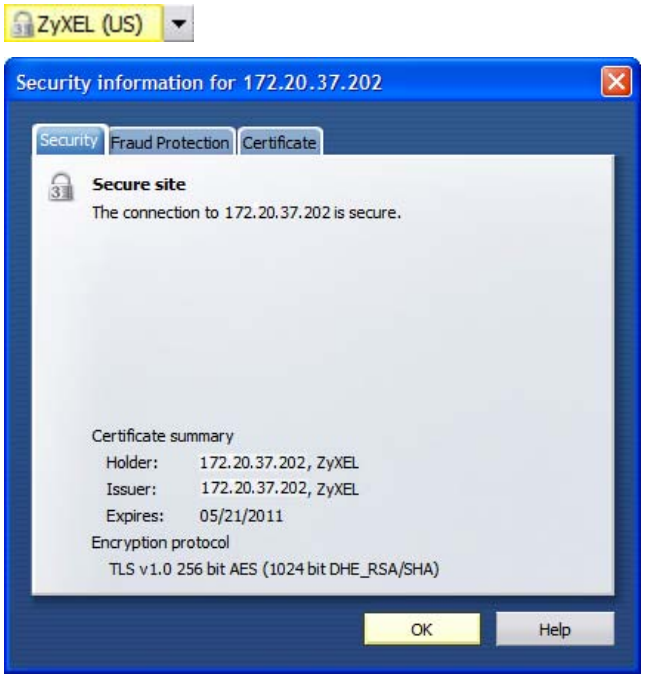
1. If your device's Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
2. Click **Install** to accept the certificate.

Figure 278 Opera 9: Certificate signer not found


Certificate signer not found
The root certificate for this server is not registered. You may install this certificate. Accept/install?
172.20.37.202
View
- The root certificate from "172.20.37.202" is not known to Opera. Opera cannot decide if this certificate can be trusted.
Accept
Install
Cancel
Help

3. The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

Figure 279 Opera 9: Security information

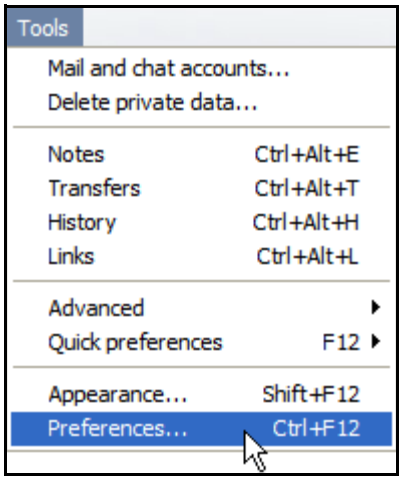


Installing a Stand-Alone Certificate File in Opera

Rather than browsing to a ZyXEL Web Configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

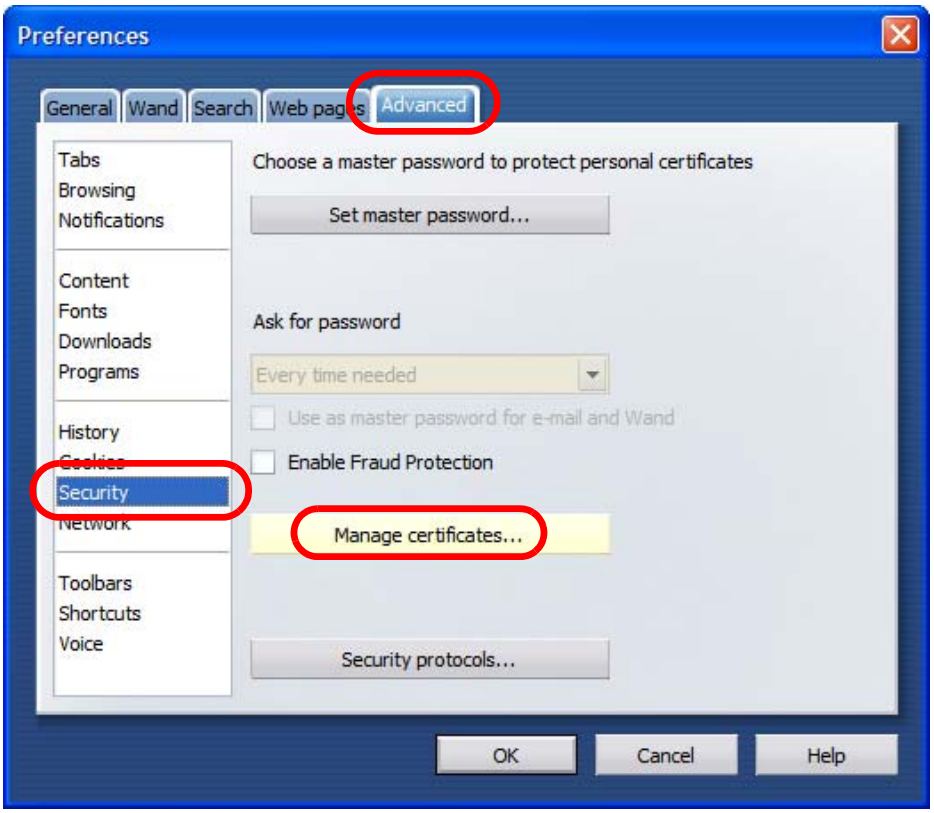
1 Open **Opera** and click **Tools** > **Preferences**.

Figure 280 Opera 9: Tools Menu



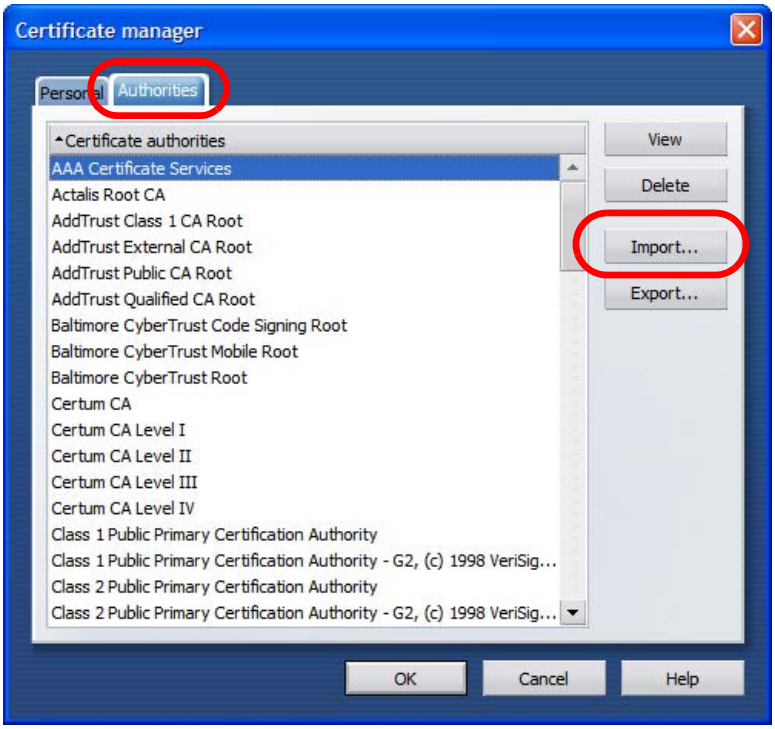
2 In **Preferences**, click **Advanced** > **Security** > **Manage certificates**.

Figure 281 Opera 9: Preferences



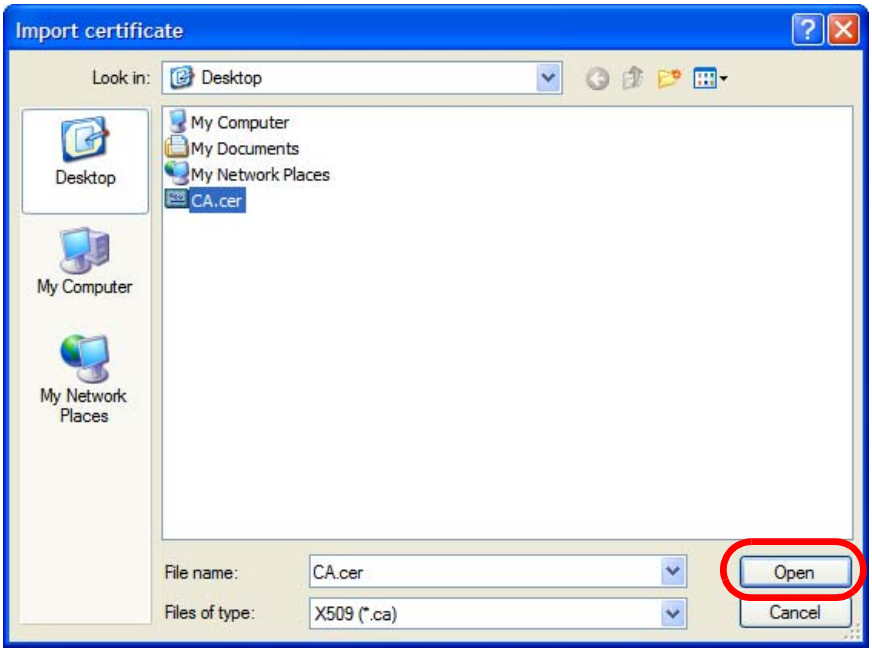
3 In the **Certificates Manager**, click **Authorities** > **Import**.

Figure 282 Opera 9: Certificate manager



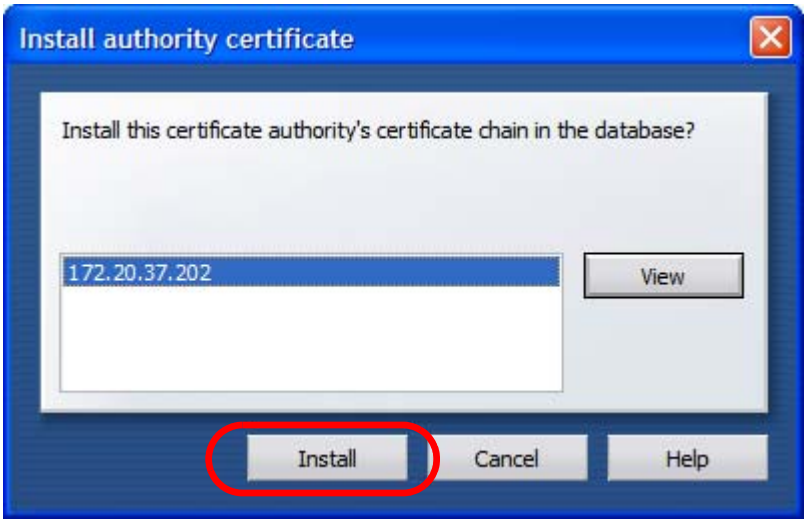
4 Use the **Import certificate** dialog box to locate the certificate and then click **Open.**

Figure 283 Opera 9: Import certificate



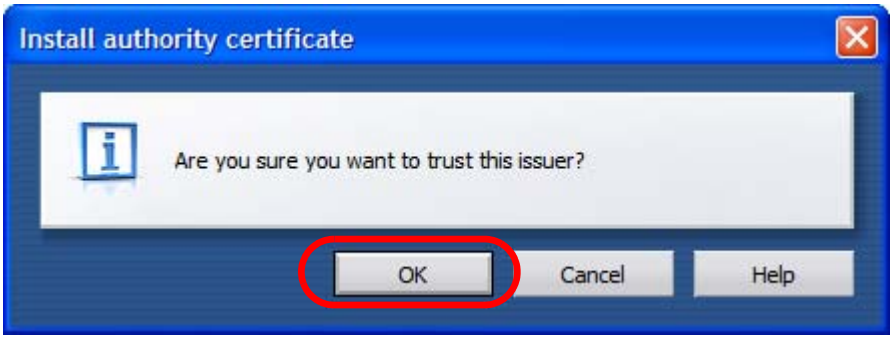
5 In the **Install authority certificate** dialog box, click **Install**.

Figure 284 Opera 9: Install authority certificate



6 Next, click **OK**.

Figure 285 Opera 9: Install authority certificate



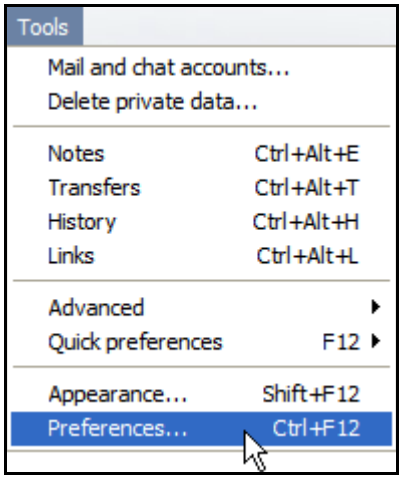
7 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

Removing a Certificate in Opera

This section shows you how to remove a public key certificate in Opera 9.

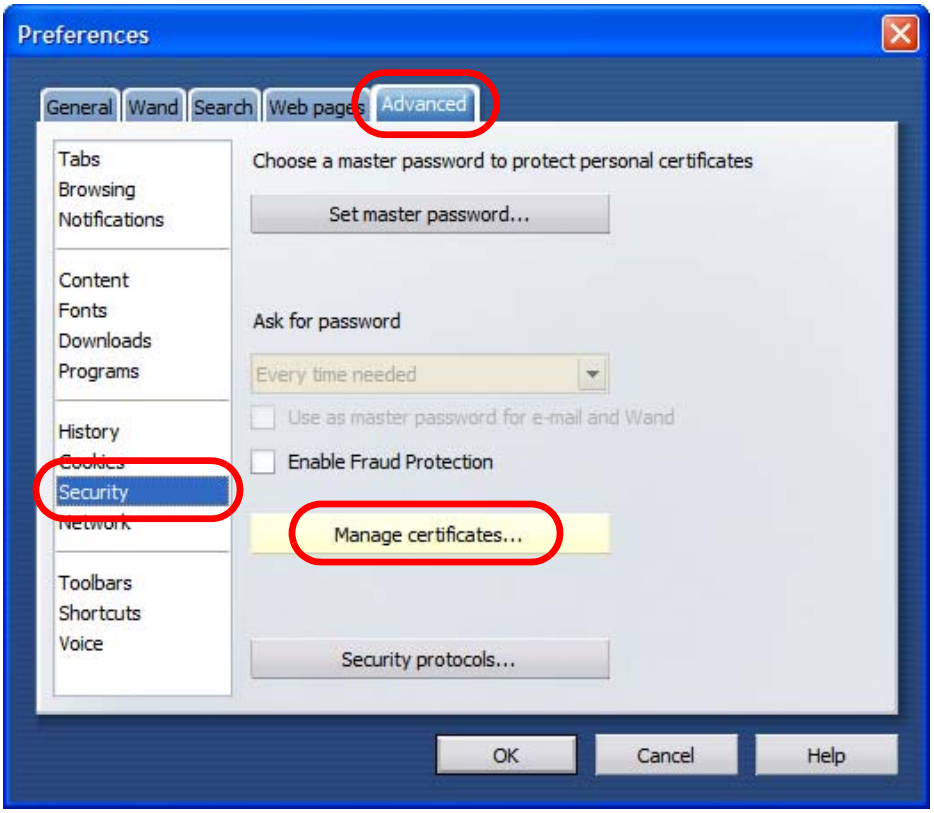
1 Open **Opera** and click **Tools** > **Preferences**.

Figure 286 Opera 9: Tools Menu



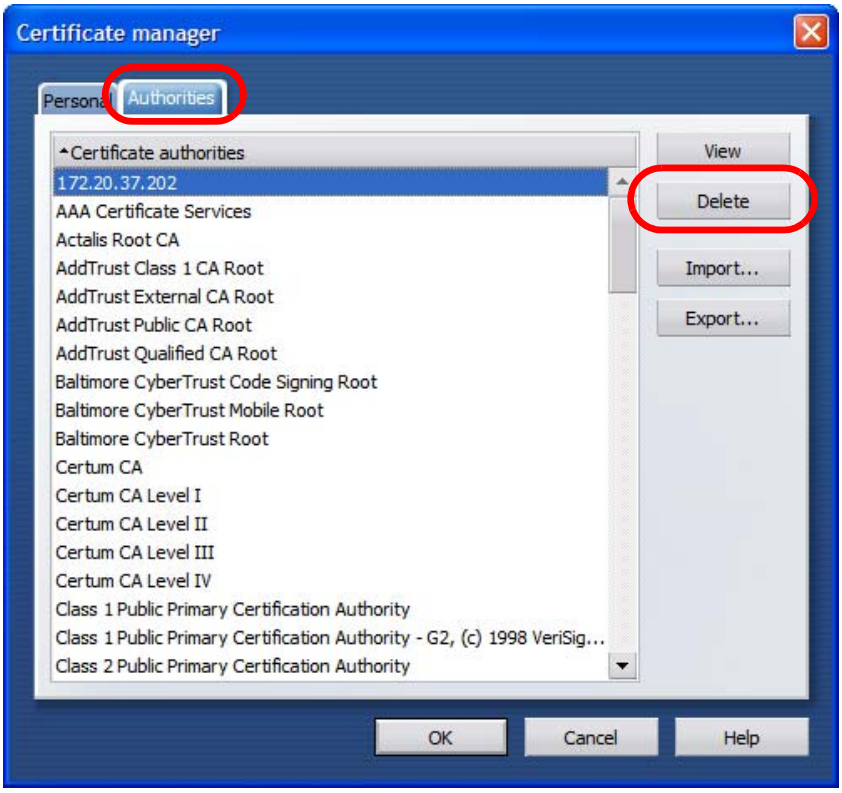
2 In **Preferences**, **Advanced** > **Security** > **Manage certificates**.

Figure 287 Opera 9: Preferences



3 In the **Certificates manager**, select the **Authorities** tab, select the certificate that you want to remove, and then click **Delete**.

Figure 288 Opera 9: Certificate manager



4 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

There is no confirmation when you delete a certificate authority, so be absolutely certain that you want to go through with it before clicking the button.

Konqueror

The following example uses Konqueror 3.5 on openSUSE 10.3, however the screens apply to Konqueror 3.5 on all Linux KDE distributions.

1. If your device's Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
2. Click **Continue**.

Figure 289 Konqueror 3.5: Server Authentication

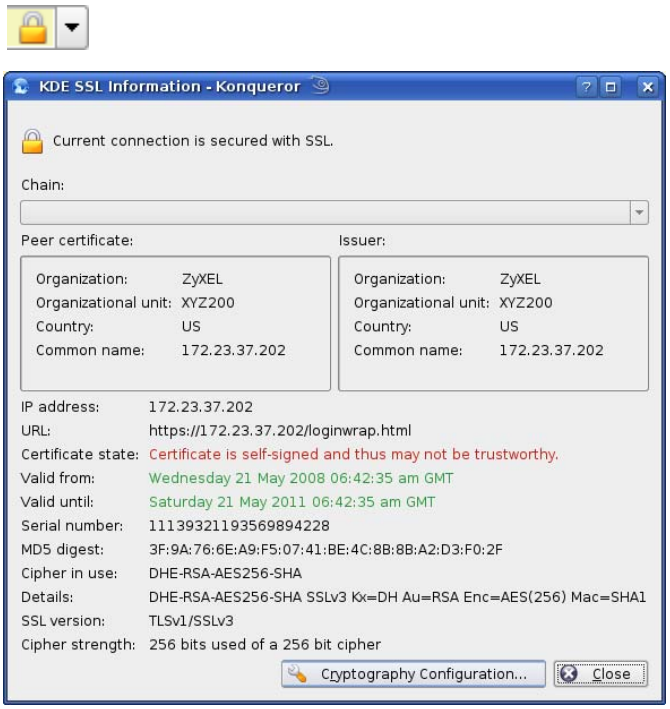
3. Click **Forever** when prompted to accept the certificate.

Figure 290 Konqueror 3.5: Server Authentication

Server Authentication - Konqueror
Would you like to accept this certificate forever without being prompted?
Forever
Current Sessions Only

4. Click the padlock in the address bar to open the **KDE SSL Information** window and view the web page's security details.

Figure 291 Konqueror 3.5: KDE SSL Information



Installing a Stand-Alone Certificate File in Konqueror

Rather than browsing to a ZyXEL Web Configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

1 Double-click the public key certificate file.

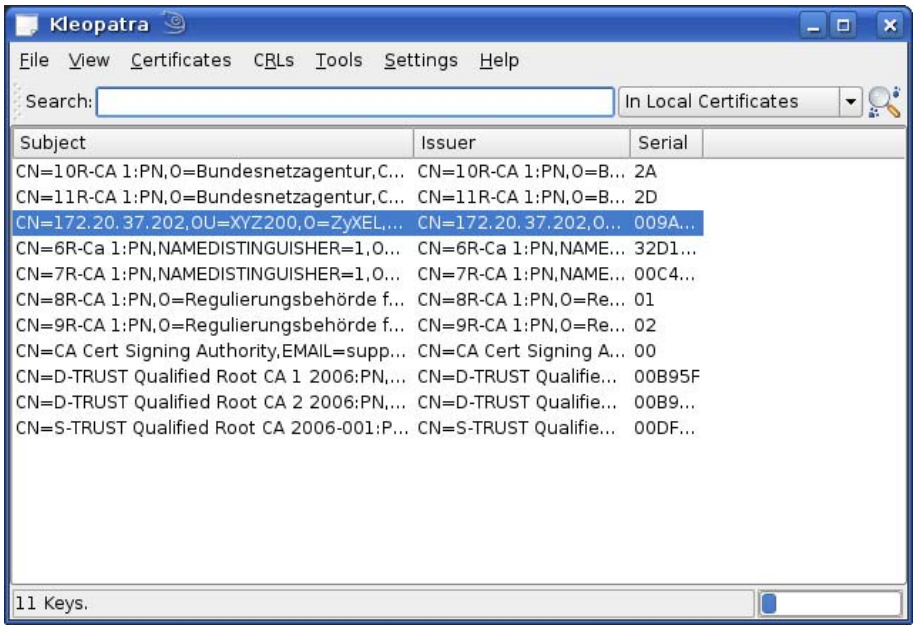
Figure 292 Konqueror 3.5: Public Key Certificate File

2 In the **Certificate Import Result - Kleopatra** dialog box, click **OK**.

Figure 293 Konqueror 3.5: Certificate Import Result

The public key certificate appears in the KDE certificate manager, **Kleopatra**.

Figure 294 Konqueror 3.5: Kleopatra


Kleopatra
File View Certificates CRLs Tools Settings Help
Search:
In Local Certificates
Subject Issuer Serial
CN=10R-CA 1:PN,O=Bundesnetzagentur,C... CN=10R-CA 1:PN,O=B... 2A
CN=11R-CA 1:PN,O=Bundesnetzagentur,C... CN=11R-CA 1:PN,O=B... 2D
CN=172.20.37.202,OU=XYZ200,O=ZyXEL,... CN=172.20.37.202,O... 009A...
CN=6R-Ca 1:PN,NAMEDISTINGUISHER=1,O... CN=6R-Ca 1:PN,NAME... 32D1...
CN=7R-CA 1:PN,NAMEDISTINGUISHER=1,O... CN=7R-CA 1:PN,NAME... 00C4...
CN=8R-CA 1:PN,O=Regulierungsbehörde f... CN=8R-CA 1:PN,O=Re... 01
CN=9R-CA 1:PN,O=Regulierungsbehörde f... CN=9R-CA 1:PN,O=Re... 02
CN=CA Cert Signing Authority,EMAIL=supp... CN=CA Cert Signing A... 00
CN=D-TRUST Qualified Root CA 1 2006:PN,... CN=D-TRUST Qualifie... 00B95F
CN=D-TRUST Qualified Root CA 2 2006:PN,... CN=D-TRUST Qualifie... 00B9...
CN=S-TRUST Qualified Root CA 2006-001:P... CN=S-TRUST Qualifie... 00DF...
11 Keys.

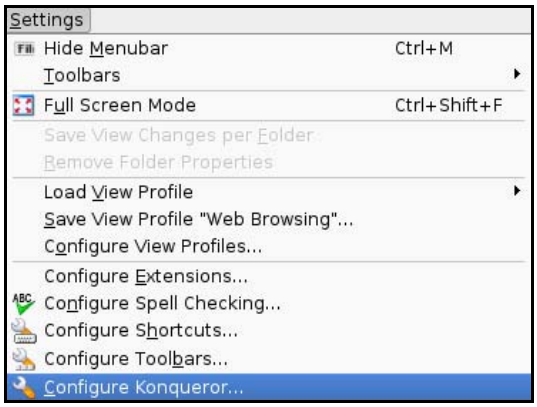
3 The next time you visit the web site, click the padlock in the address bar to open the **KDE SSL Information** window to view the web page's security details.

Removing a Certificate in Konqueror

This section shows you how to remove a public key certificate in Konqueror 3.5.

1 Open **Konqueror** and click **Settings** > **Configure Konqueror**.

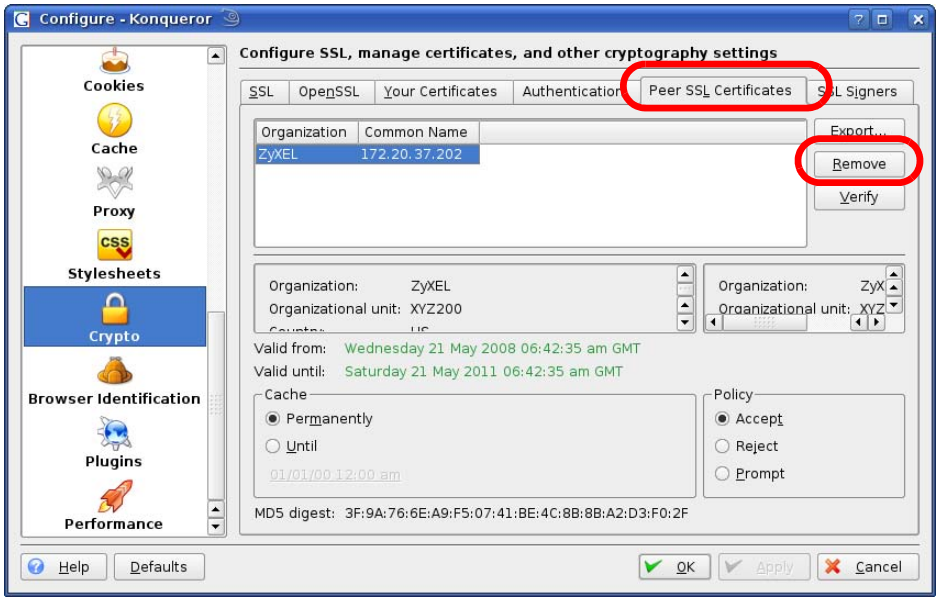
Figure 295 Konqueror 3.5: Settings Menu



2 In the **Configure** dialog box, select **Crypto**.

3 On the **Peer SSL Certificates** tab, select the certificate you want to delete and then click **Remove**.

Figure 296 Konqueror 3.5: Configure



4 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

There is no confirmation when you remove a certificate authority, so be absolutely certain you want to go through with it before clicking the button.

D

Open Source Licences

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes software developed by the Apache Software Foundation under Apache License.

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

“License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

“Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

“Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition,

“control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

“You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License.

“Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

“Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

“Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works hereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file

distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Version 1.1

Copyright (c) 1999-2003 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The end-user documentation included with the redistribution, if any, must include the following acknowledgment: “This product includes software developed by the Apache Software Foundation (http://www.apache.org/).” Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

The names “Apache” and “Apache Software Foundation” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

Products derived from this software may not be called “Apache”, nor may “Apache” appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

This Product includes phpmvc software under LGPL license.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts

as the successor of the GNU Library Public License, version 2, hence the version number 2.1.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get

it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can re-link them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the “Lesser” General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License. In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a “work based on the library” and a “work that uses the library”. The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called “this License”).

Each licensee is addressed as “you”.

A “library” means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The “Library”, below, refers to any such software library or work which has been distributed under these terms. A “work based on the Library” means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term “modification”.)

“Source code” for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library. Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) The modified work must itself be a software library. b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change. c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License. d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote

it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange. If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not

compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a “work that uses the Library”. Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a “work that uses the Library” with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a “work that uses the library”. The executable is therefore covered by this License. Section 6 states terms for distribution of such executables. When a “work that uses the Library” uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law. If such an object file uses only numerical parameters, data structure layouts and accessories, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a “work that uses the Library” with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things: a) Accompany the work with the complete corresponding

machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable “work that uses the Library”, as object code and/or source code, so that the user can modify the Library and then relent to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.) b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a

copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with. c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution. d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place. e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the

required form of the “work that uses the Library” must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things: a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above. b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to

refrain entirely from distribution of the Library. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to

contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/ donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing

and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCHDAMAGES.

END OF TERMS AND CONDITIONS.

This Product includes apcid, apcupsd, autofs, device-mapper, evms, exim. Lm_sensors, mdadm, pam_mount, raidtools, samba, sg_utils, smartmontools, vsftpd, xfsprogs and Linux kernel software under GPL license.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that re-distributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”. Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies

directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR

INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes OpenLDAP software under the OpenLDAP Public License

The OpenLDAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation (“Software”), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted

This Product includes open SSL under the Open SSL License

Open SSL License

LICENSE ISSUES
==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License
========

Copyright (c) 1998-2004 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”

The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.

Redistributions of any form whatsoever must retain the following acknowledgment:
“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related:-).

If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

“This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

This Product include mod_ssl software under BSD license

BSD

Copyright (c) [dates as appropriate to package]

The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University nor of the Laboratory may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes php software under the PHP License

The PHP License, version 3.0

Copyright (c) 1999 - 2006 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name “PHP” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.

4. Products derived from this software may not be called “PHP”, nor may “PHP” appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying “Foo for PHP” instead of calling it “PHP Foo” or “phpfoo”

5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes PHP, freely available from <http://www.php.net/>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the PHP Group.

The PHP Group can be contacted via E-mail at group@php.net. For more information on the PHP Group and the PHP project, please see <http://www.php.net>.

This product includes the Zend Engine, freely available at <http://www.zend.com>.

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This Product includes Sablotron software under MPL License

Mozilla Public License Version 1.1

1. Definitions.

1.0.1. "Commercial Use" means distribution or otherwise making the Covered Code available to a third party.

1.1. "Contributor" means each entity that creates or contributes to the creation of Modifications.

1.2. “Contributor Version” means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. “Covered Code” means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4. “Electronic Distribution Mechanism” means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. “Executable” means Covered Code in any form other than Source Code.

1.6. “Initial Developer” means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. “Larger Work” means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. “License” means this document.

1.8.1. “Licensable” means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. “Modifications” means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

Any new file that contains any part of the Original Code or previous Modifications.

1.10. “Original Code” means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. “Patent Claims” means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. “Source Code” means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. “You” (or “Your”) means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, “You” includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, “control” means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof) the licenses granted in this Section 2.1 (a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

Notwithstanding Section 2.1 (b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination) the licenses granted in Sections 2.2 (a) and 2.2 (b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

Notwithstanding Section 2.2 (b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled “LEGAL” which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or unscrupulous) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor Apes

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the legal file.

(c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3.4 (a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any

Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Sections 3.1, 3.2, 3.3, 3.4 and 3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the legal file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6. Versions of the License.

6.1. New Versions

Netscape Communications Corporation (“Netscape”) may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3. Derivative Works

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases “Mozilla”, “MOZILLAPL”, “MOZPL”, “Netscape”, “MPL”, “NPL” or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. Disclaimer of warranty

Covered code is provided under this license on an “as is” basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the covered code is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the covered code is with you. Should any covered code prove defective in any respect, you (not the initial developer or any other contributor) assume the cost of any necessary servicing, repair or correction. This disclaimer of warranty constitutes an essential part of this license. No use of any covered code is authorized hereunder except under this disclaimer.

8. Termination

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declaratory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as “Participant”) alleging that:

such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. Limitation of liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall you, the initial developer, any other contributor, or any distributor of covered code, or any supplier of any of such parties, be liable to any person for any indirect, special, incidental, or consequential damages of any character including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party's negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to you.

10. U.S. government end users

The Covered Code is a “commercial item,” as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of “commercial computer software” and “commercial computer software documentation,” as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. Miscellaneous

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. Responsibility for claims

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. Multiple-licensed code

Initial Developer may designate portions of the Covered Code as “Multiple-Licensed”. “Multiple-Licensed” means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the MPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

Exhibit A - Mozilla Public License.

“The contents of this file are subject to the Mozilla Public License Version 1.1 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.mozilla.org/MPL/

Software distributed under the License is distributed on an “AS IS” basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____.

Portions created by _____ are Copyright (C) _____

_____. All Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms of the _____ license (the “[___] License”), in which case the provisions of [_____] License are applicable instead of those above. If you wish to allow use of your version of this file only under the terms of the [____] License and not to allow others to use your version of this file under the MPL, indicate your decision by deleting the provisions above and replace them with the notice and other provisions required by the [___] License. If you do not delete the provisions above, a recipient may use your version of this file under either the MPL or the [___] License.”

NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.

This Product includes expiate and krb5 software under the MIT License

The MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

NOTE: Some components of the NSA-2401 incorporate source code covered under the Apache License, GPL License, LGPL License, BSD License, Open SSL License, OpenLDAP License, PHP License and MIT License. To obtain the source code covered under those Licenses, please contact ZyXEL Communications Corporation at: ZyXEL Technical Support.

End-User License Agreement for “NSA-2401”

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR MONEY WILL BE REFUNDED.

1.Grant of License for Personal Use

ZyXEL Communications Corp. (“ZyXEL”) grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the “Software”), including any documentation files accompanying the Software (“Documentation”), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2.Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3.Copyright

The Software and Documentation contain material that is protected by United States Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4.Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. You may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing.

5.Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6.No Warranty

THE SOFTWARE IS PROVIDED “AS IS.” TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7.Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL'S AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND

DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED $1,000. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8.Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9.Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10.Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

12.General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

E

Legal Information

Copyright

Copyright © 2009 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Index

A

about icon 48
access
  configuration 44, 189
Access Control List, see ACL
accessing share contents 40
account names 179
ACL 85, 174, 175, 190
Active Directory, see AD
active sessions 120
AD 165
add disk 137
administration screens 38, 47
ALM LED 32
  troubleshooting 250
anonymous 193
ANONYMOUS FTP 193, 253
anonymous FTP access 225
Apache License 323
Apple 31, 65
archive 96, 203
array 125
  degraded 126
  down 126
  repair 126
  resynching 134

B

backup 89, 96, 200
  archive 96, 203
  bandwidth 206
  compression 206
  create 202
  edit 208
  encryption 206
  mirror 203
  publish 203
  purge settings 207
  purging 200
  restore by files 212
  restore by job 209
  software 220
  synchronization 203
  synchronization tutorial 92
  troubleshooting 254
  tutorial 92
backup files
  restoring files by 102
backup job
  restoring files by 99
backups
  purge settings 209
  versus snapshots 199
bandwidth 206
browsers 35
browsing shares 40
BSD 340
buzzer 233
  troubleshooting 251

C

capacity 106
  using 109
certificate 229, 240
  editing 240
  tutorial 69
  verifying 79
certifications 260, 353
  notices 353
  viewing 354
change password 37
CIFS 160, 164
Comma Separated Value, see CVS
Common Internet File System, see CIFS
common screen icons 51
compatible hard disks 259
compression 206
configuration file
  backup 237
  maintenance 237
  restore 237
configuration file backup 198
conflict user 177
conflict, in 173
conflicting access settings 175
conflicting settings 175
connection limit 225

copied files folder format 33
COPY
button 33, 227
folder format 33
LED 33
share 227
COPY LED
troubleshooting 255
copying 33, 42
copyright 48, 353
CPU
temperature 119
usage 118
crypto 141, 148
CSV 236

D

date 121
daylight saving 122
default
IP address 36
password 36
settings 52
username 36
degraded
array 126
deleting
folders or files 41
RAID 136
shares 187
user accounts 176
user groups 183
volumes 140
DFS 194
DHCP 160, 258
diagnostic tool 164
disclaimer 353
disk 125
eject 129
external 145
internal 128
LEDs 32
quota 258
recommendations 132
replacement restrictions 128
S.M.A.R.T. attributes 156
see also hard drive
disk quota
conflict users 177
Distributed File System, see DFS
DNS 164
server address assignment 159
domain 177
group 173
user 173
domain controller
time 165
domain mode 258
domain name 167
Domain Name System. See DNS.
domain security mode 165
domain user
troubleshooting 253
troubleshooting share access 254
down array 126
duplexing 151
Dynamic Host Configuration Protocol, see DHCP

E

eject 146
ejecting a disk 129
EMC 260
encrypted volume
password 142, 149
encryption 126, 206
EVERYONE 193
exiting the Web Configurator 38, 49
expand JBOD 137
explicit TLS/SSL 82
export log 236
EXT2 150
EXT3 150
external
devices 39, 107
shares 39
external disk
eject 146
locate 146
external storage 145
lock 148
scan 147
unlock 148
volume 147
external volume 147
create 149
EXT2 150
EXT3 150
FAT16 150
FAT32 150
file system 150
lock 148

NTFS 150
ReiserFS 150
scan 147
unlock 148
XFS 150

F

factory defaults 52
fan speed 119
FAT16 150
FAT32 150
FCC interference statement 353
file
access 85
browsing 40
path 43
restricted 88
security 85
storage system 260
system 150
troubleshooting access 254
File Transfer Protocol over Explicit TLS, see FTPES
File Transfer Protocol, see FTP
files
deleting 41
FileZilla 81
fingerprint 79
firmware 241
specifications 260
upgrade 241
version 1, 119, 200
folder 38, 40
access 85
browsing 40
name restrictions 45
security 85
troubleshooting access 254
folders
copying 42
deleting 41
moving 42
forgot password 251
front panel LEDs 32
FTP 81, 223, 224
anonymous access 225
character set 225
connection limit 225
idle timeout
FTP 225
over Explicit TLS 81
settings 169
FTPES 81, 223
FTPES - FTP over explicit TLS/SSL 82

G

Genie Backup Manager 258
license keys 220
port conflict 198
Gigabit Ethernet 31, 257
global
icons 38, 48
labels 38
GNU GENERAL PUBLIC LICENSE 333
GNU LESSER GENERAL PUBLIC LICENSE 326
group
name restrictions 185
group names 185
groups 58, 182

H

hard drive 125
external 39
internal 39
manufacturers 31
recommendations 132
see also disk
sleep time 243
hardware specifications 259
help icon 48
home icon 49
hot spare 137, 155
HTTP over SSL, see HTTPS
HTTPS 75, 229, 239
humidity 260
hyper links 49
HyperText Transfer Protocol over Secure Socket Layer, see HTTPS

I

icons 38
about 48
administration 48
common 51
global 38, 48
help 48
home 49

logout 38, 49
user 52
web help 38
idle timeout 225
hard drive 243
in conflict 173
internal
file system 174
hard drives 39
IP address, default 36

J

JavaScript 35
JBOD 132, 152
expand 137
jumbo frames 160, 161, 164

L

LAN LEDs 33
troubleshooting 251
LAN1 36
LAN2 36
language 48
leave domain 168
LEDs
disk drive 32
front panel 32
NSA 32
troubleshooting 249
Leopard 65
liability 353
license 353
agreement 349
links, to screens 49
Linux 31
local
group 173
user 173
locate 146
lock 141, 148
external volume 148
locked volumes 126
log 230
buzzer priority 233
classes 231, 237
CSV 236
export 236
records configuration 232
report configuration 233
search 232
severity 237
logging/monitoring 261
logical volume 174
manager 174
login
troubleshooting 252
username 36
logout
automatic 37
icon 38, 49

M

Mac 65
MAC address 119
management session
timeout 37
managing
files 40
shares 43
mapping a share 61
mapping shares 61
MDI/MDI-X 257
message
text box 51
Microsoft Excel 236
migrating a RAID 110
mirror 203
mirroring 151
MIT License 348
mode
domain 177
workgroup 177
model name 48, 119
moving share contents 42
Mozilla Public License 341
My NSA 38
changing share properties screen 43
management overview screens 42
screens 37, 38
tutorial 63
My Own Shares 39

N

name details 44

NAS 174
navigation panel 49
NDU 35
  troubleshooting discovery 252
network
  connection test 164
  protocols 260
  security 260
Network-Attached Storage, see NAS
NFS 168
  share name details 170
non-admin users 180
NSA Discovery Utility, see NDU
NSA LEDs 32
NTFS 150

O

open source licences 323
Open SSL License 337, 338
OpenLDAP 337
OpenLDAP Public License 337
operating humidity 260
operating temperature 260
OS X 65

P

parity 151
password 36, 38, 46
  change screen 37
  changing 46
  default 36
  forgot? 52
Patent 353
path 43
PHP License 340
ping 164
power 89
  button 33
  consumption 261
  failure 89, 244
  restart 89
  resume 89, 244
  schedule 244
power adaptor pinout 261
power management 242
  hard drive sleep time 243
primary domain controller 258
print server 224, 226
  rename 226
  tutorial 104
printer 31
proof of purchase 354
protect 96, 197
  backup 89
  backup tutorial 92
  snapshot 89
public key certificate 229, 240
  editing 240
publish 203
purge 200
PWR LED 32
  troubleshooting 250

Q

quota for storage 178

R

RAID 31, 125, 132
  add disk 137
  background information 151
  data protection 156
  degraded 250
  down 250
  expand JBOD 137
  file storage 257
  four disks 134
  hard drives to use 132
  hot spare 137
  level 139
  levels 132
  migrating 110
  one disk 133
  quick comparison 132
  RAID 0 153
  RAID 10 154
  RAID 5 155
  RAID 5 spare 155
  remove 136
  reshape 137
  reshaping 107
  resync speed 137
  resynching 250
  resynchronizing 135
  status 134
    degraded 134

down 135
healthy 134
summary 135
three disks 134
two disks 133
recycle bin 194
Redundant Array of Independent Disks, see RAID
ReiserFS 150
related documentation 3
repair 126
replacing disks 128
reset button 257
procedure 52
reset defaults 52
reshape 137
reshaping 107
restart 246
restoring
by backup files 212
by backup files tutorial 102
by backup job 209
by backup job tutorial 99
files 99
restricted
file 190
file example 88
folder 190
restrictions
on folder names 45
on replacing disks 128
on share names 45
on volume names 45
resync speed 137
resynching 134, 250
resynchronizing a RAID 135
rights 353

S

S.M.A.R.T. 129
attributes 156
safety warnings 6
SATA 31, 257
scan
external volume 147
internal volume 140
screen
links 49
summary 49, 50
secure connections 75
security 68
Self-Monitoring, Analysis, and Reporting Technology, see S.M.A.R.T.
Serial Advanced Technology Attachment, see SATA
server name 119
share 38, 174
access 44, 83, 189, 193
anonymous access 193
browsing 40
changing properties 43
configuration 42
conflicting access settings 175
everyone access 193
file path 43
list 186
management details 39
name details 44
name restrictions 45
paths 46, 190
recycle bin 194
troubleshooting local user access 253
tutorial 59
shared folder 38
sharing 55
shut-down
procedure 33
shutdown 245
sleep time 243
smb 68
snapshot 89, 174, 257
affect on write performance 91, 218
create 218
creation 90
image access 91, 217
images 219
notes 198
restoring files 91
troubleshooting 254
versus backup 199
spreadsheets 236
SSL 82, 239
tutorial 69
standby drive 137
status
messages 51
screen 117
storage 125, 260
disk 128
external disk 145
humidity 260
increasing capacity tutorial 106
internal 127
temperature 260
striping 151
sub-links 49
supported clients 260

synchronization 203
tutorial 92
syntax conventions 4
SYS LED 33
troubleshooting 249
syslog server 229, 236
system management 261
system setting 121

T

TCP/IP 162
teaming mode 163
temperature
CPU 119
operating 260
thumbprint 79
time 121
Daylight Saving Time 122
lag 122
time server 122
timeout 37
TLS 82, 223
Transport Layer Security, see TLS
troubleshooting
backups 254
buzzer 251
COPY LED 255
domain user 253
domain user share access 254
file access 254
folder access 254
forgot password 251
LED indicators 249
ALM 250
LAN 251
PWR 250
SYS 249
local user share access 253
login 252
NDU discovery 252
non-admin passwords 252
overview 249
snapshots 254
Web Configurator access 252
tutorials 55

U

Unicode
8-bit UCS/Unicode Transformation Format, see UTF-8
unlock 140, 141, 146, 148
external volume 148
unlocked volumes 126
upgrading firmware 241
uploading files 40
UPS 243
USB 31, 107
devices 39
drives 145
eject 146
external volume 147
file system 150
key 142, 143, 149
locate 146
lock 148
scan 147
unlock 148
volume 149
user 46
access permissions 38
accounts 55
conflict user disk quota 177
conflict users 177
group names 185
groups 182
icon 52
list 175
name restrictions 179
non-admin 180
password management 46
passwords 258
quota 178
screens 37
storage quota 178
user-level screens 49
username 36
using
increased RAID capacity 109
UTF-8 45

V

volume 125, 174
choosing a storage method 133
create 142, 149
creating 138
crypto 141, 148
down 139
edit 142
encryption 126
healthy 139
lock 141

locked 126, 139
name restrictions 45
password 142, 149
RAID 1 153
scan 140
status 134
summary 139
unlock 140, 141, 146
unlocked 126, 139
USB key 142, 143, 149

W

warranty 354
period 354
web browsers
share access tutorial 62
supported 261
Web Configurator 35
browsers 35
logout 38, 49
troubleshooting access 252
web help 48
icon 38
web security 75
Windows 31
Windows domain
administrator 167
administrator password 168
leave 168
security mode 165
Windows Explorer 61
workgroup 177, 258
workgroup security mode 165
write performance 91, 218
affected by snapshots 91, 218

X

XFS 150, 174

Z

ZyXEL Communications Corporation 353
ZyXEL Limited Warranty
Note 354